

Fachhochschule Köln
Abteilung Gummersbach
Fachbereich Informatik
Studiengang Wirtschaftsinformatik

Diplomarbeit

DER EINSATZ VON ELECTRONIC COMMERCE - VERTRIEB IM INTERNET AM BEISPIEL EINER MITTELSTÄNDISCHEN FIRMA

Eingereicht von
Rebecca Okoroji

Prüfer:
Prof. Dr. Faeskorn - Woyke
Prof. Dr. Victor

Gummersbach, den 24. September 1998

Diplomarbeit: Der Einsatz von Electronic Commerce

Rebecca Okoroji

Inhaltsverzeichnis

Kapitel 1 [Vorwort](#)

- 1.1 Der Einsatz von Electronic Commerce - Vertrieb im Internet am Beispiel einer mittelständischen Firma

Kapitel 2 [Was ist Electronic Commerce?](#)

- 2.1 Das Internet
- 2.2 Electronic Commerce: Vertrieb im Internet

Kapitel 3 [Warum macht man E-Commerce?](#)

- 3.1 Globalisierung/Neue Märkte
- 3.2 Kosten
- 3.3 Gleichstellung
- 3.4 Marketing
- 3.5 Image
- 3.6 Versorgungsketten
- 3.7 Interaktivität
- 3.8 24-Stunden Service
- 3.9 Disintermediation
- 3.10 Aktualität
- 3.11 Multimedia
- 3.12 Virtuelle Sortimente

Kapitel 4 [Wer macht E-Commerce?](#)

- 4.1 Die Branche, die Produkte
- 4.2 Der Markt, die Kunden

Kapitel 5 Hemmnisse

- 5.1 Vorurteile
- 5.2 Kosten/fehlende Bandbreite
- 5.3 Zugang
- 5.4 Rechtliche Aspekte
- 5.5 Umsatzsteuer
- 5.6 Zahlung
- 5.7 Sicherheit

Kapitel 6 Wie wird E-Commerce gemacht?

- 6.1 Phasen einer Online-Bestellung
- 6.2 Vorüberlegungen
- 6.3 Wahl des Providers
- 6.4 Datenquelle
- 6.5 Implementierung
- 6.6 Design
- 6.7 Qualitätssicherung
- 6.8 Werbung (Site Promotion)
- 6.9 Pflege
- 6.10 Wichtige Funktionen eines Bestellsystems

Kapitel 7 Kohlhage Verbindungstechnik GmbH & Co KG

- 7.1 Firmenprofil
- 7.2 Kohlhage und das Internet
- 7.3 Das Bestellsystem

Kapitel 8 Wie sieht die Zukunft aus?

- 8.1 Mögliche Richtungen des Internets
- 8.2 Zahlung
- 8.3 Sicherheit
- 8.4 Technik
- 8.5 Certification Authority

Kapitel 9 Schlußwort

Anhang





Kapitel 1: VORWORT

1.1 Der Einsatz von Electronic Commerce - Vertrieb im Internet am Beispiel einer mittelständischen Firma

In dieser Diplomarbeit werden die Fragen: "Was ist es?", "Warum macht man es?", "Wer macht es?", und "Wie macht man es?" zu Electronic Commerce einmal theoretisch und dann praktisch, anhand der Erfahrungen der Firma Kohlhage Verbindungstechnik GmbH, beantwortet. Die Diplomarbeit besteht aus dieser Ausarbeitung und einer Diskette mit der neuen Website der Firma Kohlhage Verbindungstechnik GmbH.

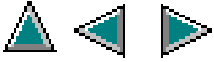
Unter Electronic Commerce kann man die Business-to-Business Verbindungen über EDI, Online-Auktionen oder auch Homebanking verstehen. In dieser Diplomarbeit untersuche ich allerdings nur den Einsatz von Electronic Commerce als Produktinformations- bzw. Bestellsystem. Da das Internet sehr dynamisch ist und sich ständig weiterentwickelt, kann diese Diplomarbeit nur ein Schnappschuß der derzeitigen Situation sein.

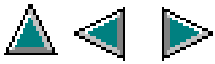
- Kapitel 2 erklärt kurz den Begriff Electronic Commerce
- Kapitel 3 erläutert weshalb Electronic Commerce immer öfter eingesetzt wird
- Kapitel 4 zeigt auf, welche Branchen und Produkte geeignet sind für den Online-Vertrieb
- Kapitel 5 listet einige Hemmnisse auf, die den Erfolg von Electronic Commerce bremsen
- Kapitel 6 erläutert die notwendigen Schritte und stellt mögliche Programmiersprachen/Werkzeuge zur Implementierung von Electronic Commerce vor
- Kapitel 7 stellt die Firma Kohlhage Verbindungstechnik GmbH & Co KG vor sowie das implementierte Bestellsystem vor
- Kapitel 8 skizziert Zukunftsaussichten von Electronic Commerce.

Hinweise zur verwendeten Literatur werden in eckigen Klammern geschrieben. [Kracke 1996] verweist z.B. auf das von Ulrich Kracke geschriebene Werk "Datenbank-Management" vom Interest Verlag das 1996 in Augsburg veröffentlicht wurde. URLs werden im Anhang D: Websites aufgelistet.

An dieser Stelle würde ich mich gerne bei meiner Familie bedanken für ihre Unterstützung. Dann möchte ich ein großes Lob aussprechen für die Fachhochschule Köln, Abteilung Gummersbach. Mein Wirtschaftsinformatik Studium empfand ich

als sehr interessant und ganz besonders innovativ und aktuell. Es war eine hervorragende Vorbereitung auf mein Berufsleben im Bereich der Informatik. Weiterhin möchte ich mich bei Prof. Dr. Faeskorn-Woyke und Prof. Dr. Frank Victor für ihre Betreuung dieser Diplomarbeit bedanken. Besonderer Dank verdient die Firma Kohlhage, speziell Herr Rainer Nettlenbusch für seinen Einsatz und seine Begeisterung für das Bestellsystem. Und, last but not least, ein großes Dankeschön an meine Kommilitonen und Freunde für ihre Unterstützung und für sehr viel Spaß!





Kapitel 2: WAS IST ELECTRONIC COMMERCE?

2.1 Das Internet

"I think that there is a world market for maybe five computers"

IBM-Vorstand Thomas Watson (1943)

Das Internet ist ein Netzwerk aus Netzwerken. Es besteht aus Millionen von Computern, die durch eine Vielzahl von Verbindungen miteinander verknüpft sind. Es hat seine Ursprünge in den späten 60er Jahren, als das amerikanische Department of Defense (DoD) ein Netzwerk als Kommunikationsmedium aufbaute, mit dem Ziel im Falle von Rechnerausfällen weiterhin Informationen austauschen zu können. Dieses Netzwerk wurde ARPAnet genannt (nach der Advanced Research Projects Agency, ein Zweig des DoD). Es verband die Computer des DoD, militärische Forschungseinrichtungen und ein paar Universitäten. Als weitere Universitäten auch aufgenommen werden wollten, teilte das DoD das ARPAnet 1983 in das MILnet für militärische Stellen und das neue ARPAnet für nichtmilitärische Stellen auf. Das NSFnet wurde 1986 von der National Science Foundation ins Leben gerufen als der Verkehr auf dem ARPAnet explodierte und die angebotenen Dienste kurz vor dem Zusammenbruch standen, weil das Netz nicht für so eine große Datenmenge ausgelegt war. Das neue Netz ersetzte nach und nach das ARPAnet bis dieses 1990 stillgelegt wurde. 1991 hob das NSF das Verbot der kommerziellen Verwendung des NSFnets auf. Zur gleichen Zeit begannen einige Firmen, sich am Netz zu beteiligen und die ersten kommerziellen Internet-Provider fingen an, Internet-Zugänge zu verkaufen. Damit war das Netz nicht mehr nur den militärischen und akademischen Kreisen vorbehalten. Das NSFnet verschwand als die ersten kommerziellen Netzwerke wie das IBM-Netzwerk erschienen [Levine 1995, S. 49-50]. 1992 wurde erstmals das World Wide Web (WWW) implementiert. Das Internet wie wir es heute kennen wurde geboren.

Die Anzahl der im Netz stehenden Rechner kann man ermitteln. Aber nicht wieviel Leute das Internet letztendlich benutzen. Waren es im Oktober 1990 noch 313.000 eingebundene Computer weltweit, so sind es heute (Stand: 01/98) 29.670.000 [NW 1998]. Laut der RIPE NCC gab es in Deutschland 3.384 Hostrechner in Oktober 1990. Heute sind es 1.287.641 (Stand 04.07.98) [RIPE 1998]. Man schätzt, daß durchschnittlich zehn Nutzer auf einem Hostrechner zugreifen.

Das unglaublich schnelle Wachstum des Internet bzw. die rasante Zunahme der Anzahl der Nutzer (Netizens) macht das Internet für viele Unternehmen wirtschaftlich

interessant.

2.2 Electronic Commerce: Vertrieb im Internet

Electronic Commerce bedeutet soviel wie "Elektronischer Handel". Auch "Internet Business", "Electronic Business", "E-Business" oder "E-Commerce" genannt.

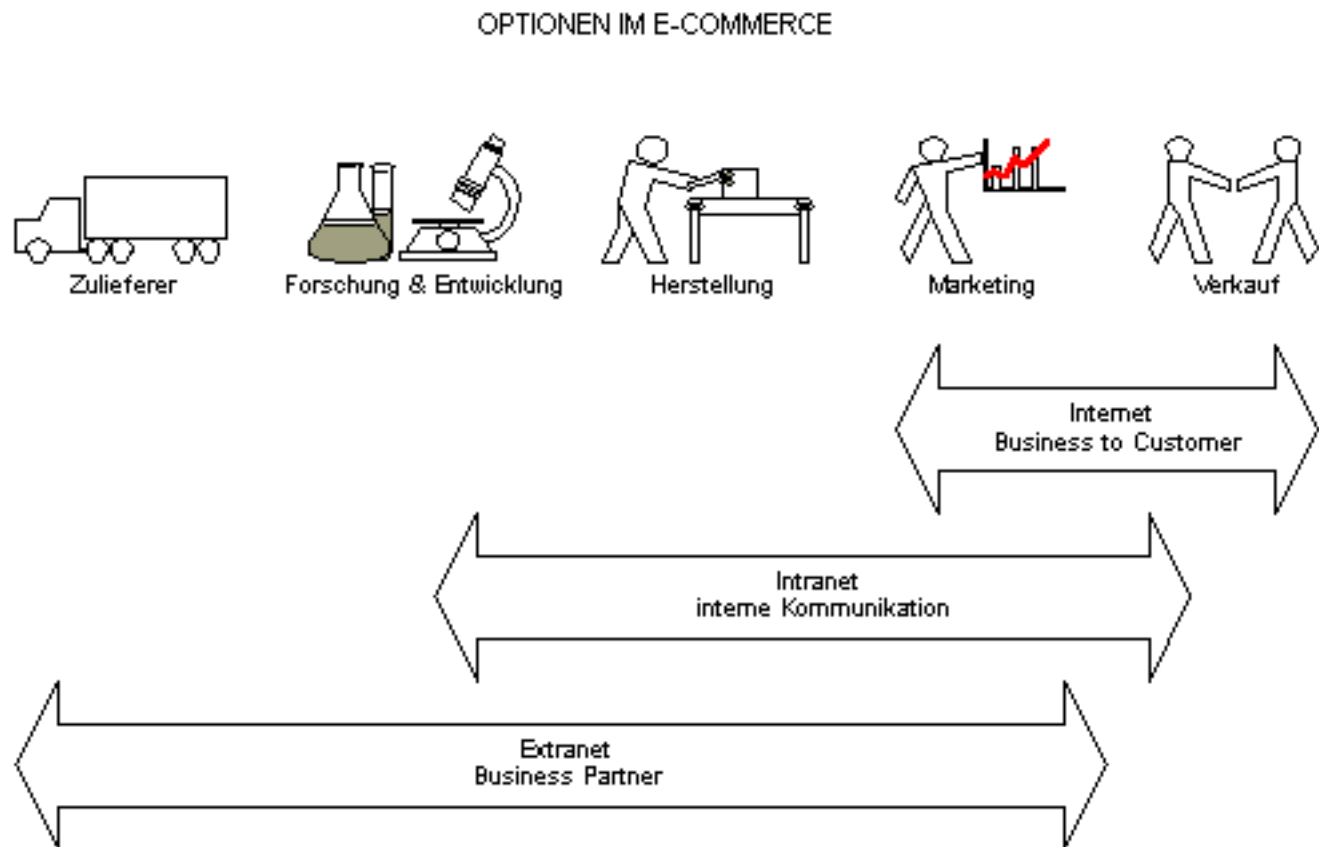


Abbildung 1: Optionen im E-Commerce

"E-Commerce bezeichnet die Ausnutzung der technischen Mittel elektronischer Datennetze, um die Wirtschafts- und Absatzprozesse einer Unternehmung zu fördern und neue Absatzwege zu erschließen. Die Einzelziele erstrecken sich dabei von der Unternehmenskommunikation über die Wertschöpfungsprozesse bis zum Verkaufsvorgang über alle Marktphasen." [Fochler 1998, S. 20]

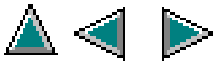
Das Intranet ist ein unternehmensinternes Netz, daß aufgebaut wird um die Informationsversorgung der Mitarbeiter zu verbessern. Ein Extranet dagegen, ist ein Kommunikationsnetz, daß ein Unternehmen mit seinen Geschäftspartnern verbindet.

Das Internet diene in den letzten Jahren vor allem der Unternehmenspräsentation. Der enorme Zuwachs von Nutzern aber macht das Internet zu einem mächtigen Medium mit dem man schnell und relativ günstig eine sehr große Zielgruppe erreichen kann. E-Commerce bietet einen neuen Absatzweg der eine vollkommene Integration von Marketing, Absatz und Service in ein elektronisches Medium erlaubt.

Über das Internet können Käufer und Verkäufer, Hersteller und Abnehmer ihre

Produkte/Dienstleistungen anbieten oder beziehen, wobei es irrelevant ist, ob der Geschäftspartner im gleichen Ort oder am anderen Ende der Welt sitzt.

Shareware war das erste Produkt, das online vertrieben wurde. Hersteller von Shareware erlauben potentielle Kunden ihre Software aus dem Internet zu beziehen und zu testen, bevor eine endgültige Kaufentscheidung gefällt wird. Solange die Software nicht registriert ist, hat sie oft nur eine beschränkte Nutzungszeit oder aber einen beschränkten Funktionsumfang. 1994 nahmen dann die ersten Einkaufszentren im Internet, sogenannte "Internet Malls", den Betrieb auf und Pizza Hut ermöglichte erstmals das Bestellen von Pizzas im Internet [Dreyer 1998, S. 5].





Kapitel 3: WARUM MACHT MAN ELECTRONIC COMMERCE?

Jeder Online-Anbieter¹ verspricht sich etwas von seinem Online-Auftritt, sei es nur aus Image-Gründen oder auch weil seine Konkurrenz es auch macht. Eine Untersuchung unter 500 Unternehmen in Deutschland hinsichtlich deren Verwendungszweck des Internets (von Juni bis September 1997) ergab folgende Ergebnisse:

| Bereitstellung von Informationen | % | Verwendung von Informationen | % |
|---|----------|--------------------------------------|----------|
| Unternehmensdarstellung | 84,3 | Informationsbeschaffung allgemein | 90,6 |
| Produktdarstellung | 76,3 | Beschaffung von Produktinformationen | 79,3 |
| Anbahnung von Geschäftskontakten | 64,2 | Anbahnung von Geschäftskontakten | 55,0 |
| Werbung für andere Unternehmen | 38,4 | Private Nutzung | 55,2 |
| Verkauf über das Internet | 34,8 | Elektronische Bestellung | 43,6 |
| | | Personalakquisition | 17,8 |
| Andere | 9,8 | Andere | 3,7 |

Tabelle 1: Zweck der WWW-Nutzung

Offenbar nutzen die Unternehmen das Internet vorwiegend in den Bereichen Marketing und Verkauf als zusätzliche Werbeplattform. Auf die Frage nach den beobachteten Nutzeffekten steht mit Abstand (68,1 %) die relativ allgemeine Position "Verbesserung des Images". Die anschließend am häufigsten genannten Nutzeffekte lassen darauf schließen, daß das Internet-Engagement direkte wettbewerbsrelevante Wirkungen hat. So sind etwa im oberen Drittel kundenbezogene Faktoren sehr stark repräsentiert: "Verbesserter Kundenservice" (52,1 %), "schnelleres und flexibleres Reagieren auf Kundenwünsche" (39,7 %), "höhere Kundenzufriedenheit" (36,2 %), "stärkere Kundenbindung" (34,2 %). Generelle marktorientierte Wirkungen fallen ebenso auf: "Neue Geschäftspartner gewonnen" (50,3 %), "Differenzierung im

Wettbewerb" (43,1 %), "neue Märkte erschlossen" (38,4 %) oder "allgemein Marktvorteile erreicht" (34,4 %). Die "höhere Flexibilität und Reaktionsfähigkeit", die etwa ein Drittel der Antwortenden nannte, können ebenfalls der Kategorie Wettbewerbswirkungen zugerechnet werden [Kurbel 1998].

3.1 Globalisierung/Neue Märkte

Ein wichtiger Aspekt liegt in der globalen Erschließung neuer Märkte. Geographische Einschränkungen entfallen und der Online-Anbieter kann seine Produkte einfach über seine Website überall auf der Welt anbieten. Wenn der Euro kommt, fallen die sich ständig ändernden Wechselkurse innerhalb Europas weg und die europäischen Märkte wachsen zusammen. Das Internet bietet dann die ideale Plattform zur Abwicklung des Bestellwesens. Natürlich verstärkt dies auch die internationale Konkurrenz.

3.2 Kosten

Dem Vertrieb über das Internet entspricht ein Geschäft, das als rein virtueller Verkaufsort nicht mehr Platz benötigt als ein Kühlschrank. Da ein realer Laden wegfällt, erspart sich der Anbieter die Kosten für Lager, Miete, Unterhalt und teilweise auch für Personal. Zusätzlich entfällt die Gefahr von Einbrüchen, Überschwemmungen, Bränden etc. und die Kosten für die damit verbundenen Versicherungen. Das Internet dient als neuer Vertriebsweg der nur minimale Investitionen verlangt.

Auch wenn der Kunde nichts bestellt, dient das Online-Angebot immer noch als Produktkatalog mit dessen Hilfe er sich über die Produkte informieren kann. Die Kosten für den Druck und den Versand von Katalogen liegen auch wesentlich höher als die für das Betreiben einer Website.

Letztlich können speziell die Softwarehersteller die Kosten für Datenträger und Handbücher sparen wenn sie ihre Software über das Internet vertreiben.

3.3 Gleichstellung

Kleine Firmen haben die gleichen Chancen wie große. Wer vorher Kundenkreise erweitern wollte, mußte neue Filialen eröffnen oder Kataloge verschicken. Mit E-Commerce können sie mit relativ geringen Investitionen neue Zielgruppen erreichen.

"Im 21. Jahrhundert gewinnen nicht die Großen, sondern die Schnellen" [Dreyer 1998, 9.4.2 S. 2].

3.4 Marketing

Ein weiterer Grund für E-Commerce ist das Marketing. Ein Online-Produktkatalog ist in der Regel sehr umfangreich. Aber das Medium Internet erlaubt es dem Kunden mit einigen wenigen Klicks genau die Produkte zu erreichen, die ihn interessieren. Der Online-Anbieter verfolgt, wer wann welche Produkte wie oft wie lange und in Zusammenhang mit welchen anderen Produkten nachgefragt hat². Das dynamische Online-Angebot paßt sich dann den Bedürfnissen bzw. Interessen des Kunden an.

Diese Marketing-Form wird "One-To-One Marketing" genannt. Kunden werden nicht grob in Abnehmergruppen klassifiziert. Der Anbieter bietet jetzt jedem Kunden ein auf ihn individuell abgestimmtes Sortiment an. Das Sortiment kann z.B. komplementäre Güter zu den Ausgewählten beinhalten. Je besser dem Anbieter diese Vorselektion gelingt, desto höher die Anpassung an die tatsächlichen Bedürfnissen des Kunden.

Es ist auch denkbar, daß der Anbieter relevante Informationen anbietet (z.B. Kochrezepte passend zu den gekauften Lebensmittel). Der Clou ist der Mehrwert des Angebots. Der zufriedene Kunden empfiehlt das Unternehmen dann auch weiter.

3.5 Image

"It's no longer a question of should you be on the Net. Yes, businesses need to be there. Because when people want information on your product, they're going to go to the Web." Geri Spieler³.

Es ist eine Frage des Images. Eine Firma im Internet zeigt sich als technologisch aufgeschlossenes Unternehmen. Zukünftige Geschäftspartner oder auch Bewerber informieren sich über die Website einer Firma. Es ist die neue Visitenkarte einer Unternehmung.

3.6 Versorgungsketten

"Nutzen Sie das WWW, um Ihren Lieferanten Zugriff auf die Lagerverwaltung zu geben, stellen Sie dann die Verbindung zum Bestellwesen her - und schon haben Sie eine Versorgungskette, die sich selbst verwaltet. Ihr Lager ist bedarfsgerecht sortiert. Sie sparen Zeit, verringern die Administration und erhöhen den Gewinn." [IBM 1998]

Der Vorgang der Kundenbestellung kann weitgehend (ausgehend vom Endverbraucher zum Hersteller) automatisiert werden. Geschäftsprozesse werden unternehmensübergreifend rationalisiert. Herkömmliche Kommunikationsmedien wie die Post, das Telefon und das Fax werden ersetzt.

3.7 Interaktivität

Das Internet ist ein interaktives Medium. Ein Bestellsystem kann dem Kunden Vorschläge machen oder Alternativen nennen, abhängig vom Inhalt der Bestellung. Der Kunde füllt sein Warenkorb mit den Produkten und kann die ganze Zeit den Gesamtpreis überwachen. Eingeräumte Kunden-Rabatte können jederzeit mit berücksichtigt werden. Dieser verändert sich mit jedem neuen Produkt und jeder Entnahme eines Produkt. Das gibt's in keinem realen Supermarkt.

3.8 24-Stunden Service

Das Schlüsselwort ist Service. Das Internet bietet einen 24-Stunden Service. Öffnungszeiten werden irrelevant. Ladenschlußzeiten gibt es nicht im Internet. Der Kunde kann sein Kaufwunsch unverzüglich befriedigen. Dies sollte mit einer schnellen Auslieferung gekoppelt sein. Wenn der Händler das Online-Bestellsystem in seine Geschäftsprozesse optimal integriert hat, kann der Kunde z.B. die Bestände und die Lieferfristen für die Produkte abfragen. Eine Eingangsbestätigung der Bestellung sollte möglichst unmittelbar per E-Mail verschickt werden. Jeder kann heute schon online Last-Minute-Reisen buchen oder Blumen für vergessene Geburtstage verschicken lassen. Die Firma [Deshima](#) stellt beispielsweise CDs nach den Wünschen des Käufers zusammen.

3.9 Disintermediation

Disintermediation bedeutet das Ausschalten von Zwischenhändlern. Das Internet bietet sich für Hersteller geradezu an, um direkt an Endverbraucher zu verkaufen. So kann der Hersteller den tatsächlichen Bedarf der Kunden selber ermitteln. Er erhöht seine Handelsspanne. Wenn er diesen Preisvorteil teilweise an seine Kunden weitergibt, steigt die Attraktivität seines Angebotes. Und für den Kunden ist der Hersteller eines Produktes in der Regel oft der beste Ansprechpartner.

3.10 Aktualität

Im Vergleich zu Printmedien, Videotext, TV-Werbung, Plakaten usw. kommt ein Teil der Attraktivität des WWW daher, daß die dort angebotenen Informationen weltweit zur Verfügung stehen und daß sie wesentlich schneller und einfacher aktualisiert werden können. Die Infos sind zum Zeitpunkt des Aufrufes immer aktuell. Zeitliche Verzögerung durch Drucken und Versenden entfallen. Aktualisierungen und Korrekturen lassen sich leicht durchführen. Produkte können schnell als Sonderangebote klassifiziert werden und zu günstigeren Preisen angeboten werden.

3.11 Multimedia

Das Internet bietet sich als Plattform für Multimedia geradezu an. Eine Unternehmung kann ihr Online-Angebot mit Video- und Audiodateien attraktiver und informativer gestalten. Inzwischen werden Musikdateien auch im Internet vertrieben.

3.12 Virtuelle Sortimente

Der Online-Anbieter kann sein Sortiment erweitern um Produkte die er nicht zwingenderweise auf Lager hat. Diese kann er dann auf Kundenwunsch hin bestellen.

¹Firmen, die eine Internet-Präsenz anbieten

²Siehe auch [Anhang B: Cookies](#). Das Protokollieren der Schritte des Kunden auf einer Website ist sehr umstritten.

³Ein Electronic Commerce Analyst der Gartner Group





Kapitel 4: WER MACHT E-COMMERCE?

Einfache Antwort: *Jeder* macht es.

Als Electronic-Commerce-Pionier gilt der Buchhändler Amazon (www.amazon.com) (seit Juli 1995 online) mit einem Nettoumsatz im letzten Quartal von 66 Millionen Dollar [c't 6/98, S. 163]. Neben dem riesigen Angebot von 3 Millionen Titeln mit umfangreichen Zusatzinformationen zu fast jedem Eintrag (z.B. Lesermeinungen und Kritiken) bietet Amazon noch Suchfunktionen über vielfältige Kategorien, ein Geschenkservice, automatische Benachrichtigung über neue Titel des Lieblingsautors usw. Die Bücher werden nicht vor Ort gelagert, sondern bei Bedarf elektronisch bei den Grossisten angefordert die diese direkt an den Kunden verschicken. Kosten für Lagerung entfallen komplett.

Auch der Computer-Händler Dell (www.dell.com) verzeichnet große Umsätze im E-Commerce-Bereich. Auf der Dell Website kann der Nutzer sich seinen gewünschten Rechner aus der großen Auswahl der angebotenen Einzelteile selbst zusammenstellen. Dell verkauft jeden Tag Rechner im Wert von fast 6 Millionen Dollar via Internet [CZ 34 (2) 1998, S. 8].

Die relative einfache Realisierung einer Online-Präsenz erzwingt und ermöglicht eine Markttransparenz für die Konkurrenz sowie auch für die Kunden.

4.1 Die Branche, die Produkte

Von lebenswichtiger Bedeutung ist der Schritt ins Internet vor allem für die Unternehmen, deren traditionelle Märkte durch die gravierende Änderungen infolge der zunehmenden Verbreitung des Netzes wegzubrechen drohen. Das sind beispielsweise Unternehmen aus den Branchen Reisebüros, Ticketverkauf, Kartenverkauf, Versandhandel, Einzelhandel und besonders Softwarehandel. Produkte die keinen Kundendienst benötigen oder nicht allzu komplex sind, eignen sich besonders für den Online-Vertrieb. Gut laufen außerdem Bücher, Musik-Cds und Videos, Flugtickets, Mietwagen, Bahnreisen und Beherbergungen. Informations-Anbieter finden im Internet einen neuen Markt. Die immateriellen Leistungen können sofort geliefert werden und eignen sich daher sehr für den Online-Vertrieb. Beispiels sind Preisvergleiche, Studien, Routenplanung, Anzeigen oder auch Telefonverzeichnisse. Eine ganz neue Branche, die sich mit der Weiterentwicklung von E-Commerce etablieren wird, ist die der sogenannten Certification Authorities¹.

Für Nischenprodukte ist der Online-Vertrieb eine Möglichkeit, den Markt zu

vergrößern. Für Nichtnischenprodukte wird dem Kunden das Beziehen der Ware erleichtert.

Abbildung 2 zeigt die Verteilung der Online-Präsenzen nach Wirtschaftszweigen, wie sie in einer Umfrage im Auftrag der Zeitschrift [Business-Online](#) festgestellt wurde.

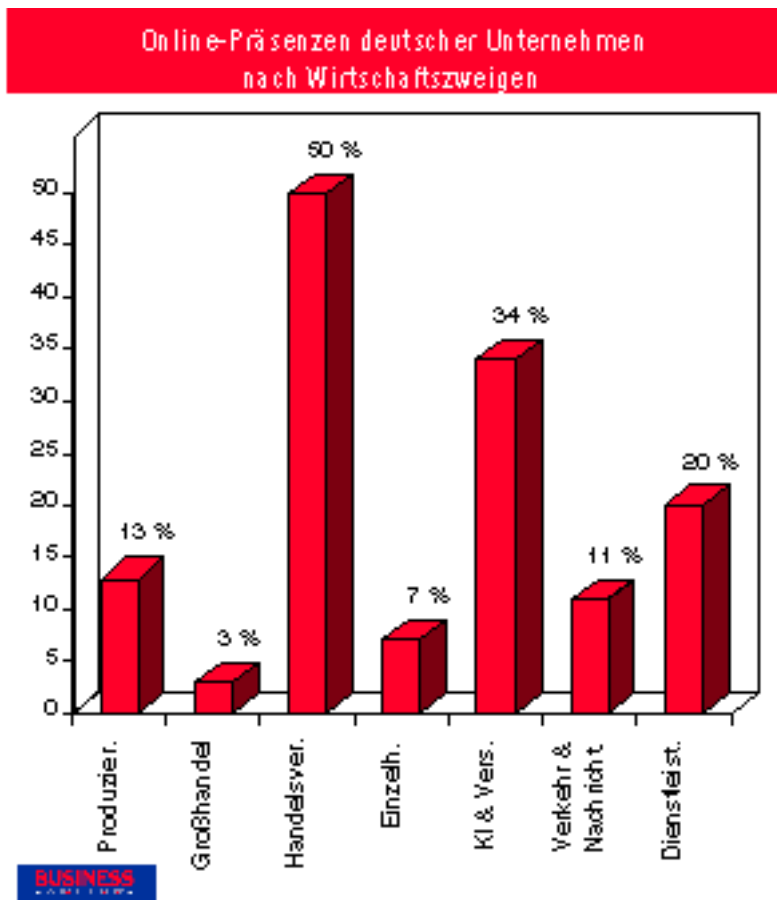


Abbildung 2: Verteilung der Online-Präsenzen auf die Wirtschaftszweige

Ungeeignete Produkte sind also solche die:

- Heterogen, nicht standardisiert und sehr kundenspezifisch sind (Einzelfertigung)
- Intensive persönliche Beratung erfordern
- Ein hohes Investitionsvolumen beim Kunden erfordern
- Unverhältnismäßig hohe Versandkosten verursachen
- Eine persönliche Begutachtung des Kunden erfordern
- Aufgrund rechtlicher Vorschriften ungeeignet sind, z.B. solche mit Altersbeschränkungen bei der Abgabe [Dreyer 1998, 9.4.2, S. 2 f.]

4.2 Der Markt, die Kunden

Die Website eines Online-Anbieters kann an Endverbraucher oder an andere Firmen gerichtet sein. Für den "Business-to-Customer" Bereich ist es zwar wichtig viele Surfer auf die Internetpräsenz zu locken aber noch wichtiger ist es, die Personen anzusprechen die sich auch tatsächlich für das Angebot interessieren. Die WWW-

Benutzer sind von der Zusammensetzung her möglicherweise der interessanteste Massenmarkt, den es überhaupt gibt. Die meisten Anwender sind männlich, zwischen 16 bis 40 Jahre alt, haben Abitur, sind oft studiert, verdienen überdurchschnittlich oder werden bald überdurchschnittlich verdienen [Fochler 1998, S. 66]. Wer bestimmte Zielgruppen ansprechen möchte, muß zunächst klären ob diese jetzt oder in Zukunft unter den Internet-Nutzern repräsentiert sind. Umfragen zu diesen Themen werden von diversen Stellen durchgeführt und veröffentlicht. In Europa führt die W3B Organisation regelmäßig Umfragen unter den Internet-Nutzern durch.

Zwischen dem 8. April und dem 27. Mai 1998 wurden alle europäischen Internet-Nutzer aufgerufen, an der 6. W3B-Umfrage² teilzunehmen. Der Fragebogen konnte in insgesamt neun Sprachen abgerufen werden (dänisch, deutsch, englisch, französisch, holländisch, italienisch, norwegisch, schwedisch und spanisch). Insgesamt haben über 16.000 Personen den Fragebogen ausgefüllt: So ist das durchschnittliche Alter der deutschsprachigen WWW-Nutzer mittlerweile auf 35,5 Jahre angestiegen; im Herbst 1997 lag es noch bei 33 Jahren. Auch der prozentuale Anteil der internet-nutzenden Frauen nimmt nun etwas schneller zu. Er beträgt heute 15,5%; bei der W3B-Herbst-Umfrage waren es noch 12,2%. Insbesondere in jüngeren Nutzergruppen finden sich überproportional viele Frauen, die erst im vergangenen halben Jahr das WWW für sich entdeckt haben.

Die 5. W3B-Umfrage fand vom 8. Oktober bis zum 19. November 1997 statt. Innerhalb dieses Zeitraums füllten 16.403 WWW-Nutzer den Fragebogen aus. Im folgenden finden sich zwei Tabellen mit den Ergebnissen zu den Fragen über das Online-Shopping.

"Haben Sie die Absicht, das WWW im nächsten halben Jahr zum Shopping zu benutzen?"

| % | Antwort |
|----------|--|
| 27,6 | Ja, bestimmt |
| 41,9 | Vielleicht |
| 8,7 | Nein, ich wüßte nicht, was ich kaufen sollte |
| 15,0 | Nein, das interessiert mich nicht |
| 1,0 | Nein, damit habe ich schlechte Erfahrungen gemacht |
| 5,9 | Weiß nicht |
| 100,0 | <i>Gesamt</i> |

Tabelle 2: WWW zum Shopping nutzen

Frage an Personen, die bereits einmal online eingekauft haben: "Waren Sie zufrieden mit dem Einkaufen via WWW?"

| % | Antwort |
|-------|---|
| 69,9 | Ja, ich werde in Zukunft öfter online einkaufen |
| 20,2 | Ja, aber ich werde in Zukunft nicht so oft online bestellen |
| 1,6 | Ja, aber ich werde es wahrscheinlich nicht wieder tun |
| 8,2 | Nein |
| 100,0 | <i>Gesamt</i> |

Tabelle 3: WWW erneut zum Shopping

Für den "Business-to-Business" Bereich liegen die Chancen höher, daß die Kunden über einen Internetzugang verfügen und diesen auch für die Online-Bestellung nutzen würden. Außerdem bestehen recht genaue Vorstellungen mit welchen Firmen kooperiert werden soll und die Vertrauensfragen sind daher nicht so kritisch. Daniel Burgwinkel, Analyst bei Diebold, rechnet daß künftig 60 Prozent der Transaktionen im Business-to-Business über Extranets abgewickelt wird. Boeing stellt beispielsweise via Extranet über 400 000 Ersatzteile für 700 Kunden bereit [CZ 28 1998, S. 25].

¹siehe auch [Kapitel 8.5 Certification Authority](#)

²Es handelt sich hierbei um freiwillig ausgefüllte Fragebögen und kann somit nicht als repräsentativ betrachtet werden. Zusätzlich ist es möglich, daß absichtlich Falschangaben gemacht werden, von kommerzfeindliche Surfer z.B.





Kapitel 5: WAS HEMMT DEN EINSATZ VON E-COMMERCE?

5.1 Vorurteile

Die Gewerkschaft HBV (Handel, Banken, Versicherungen) befürchtet, daß in den nächsten Jahren 100.000 Arbeitsplätze im Kreditgewerbe durch das Internet und Online-Dienstleistungen wegfallen könnten. Das würde etwa jedem 7. Arbeitsplatz entsprechen. Andere Untersuchungen sprechen von 100.000 - 150.000 gefährdeten Stellen im Einzelhandel durch E-Commerce.

Noch ist es allerdings noch nicht so weit, und über die Zuverlässigkeit solcher Aussagen herrscht auch unter Experten keine Einigkeit. Im Gegenteil: Nach anderen Studien können die neuen Dienstleistungsangebote im Internet bis zu 750.000 Stellen schaffen. Wer recht behält, bleibt abzuwarten [Stolpmann 1997, S. 15].

5.1.1 Kriminalität

Das Internet hat in den letzten Monaten in Deutschland einen sehr schlechten Ruf bekommen. Kinderpornographie und Rechtsradikalismus scheinen in den Köpfen der Menschen zwangsläufig mit dem Internet verbunden zu sein. Die alarmierten Medienberichte erzeugen die Vorstellung, im Internet seien diese Bereiche stark repräsentiert. Daher ist das Internet für Otto Normalverbraucher ohne Internet-Kenntnisse "böse". Berichte über die Nutzen des Internets erscheinen auch meistens nur in einschlägigen Fachzeitschriften und -sendungen und diese werden in der Regel nicht von Computer-Laien gelesen bzw. gesehen.

Heise Online, der Deutsche Kinderschutzbund, das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung, Spiegel Online und Stern Online haben die Aktion "Netz gegen Kinderporno" gestartet. Ziel dieser Aktion ist der Unterstützung der Bekämpfung der Kinderpornographie im Internet [c't 16/98, S. 16 f].

5.1.2 Der "Gläserne Kunde"

Die "Horrorvision": der gläserne Kunde, dessen Angewohnheiten dokumentiert wird um ein Kunden-Profil zu erstellen. Das ist ein weiteres Vorurteil welches den Einzug von E-Commerce hemmt. Cookies¹ werden als Instrumente zur Überwachung, ("big brother's watching") empfunden. Surfer befürchten, daß sie nicht mehr anonym

durchs Internet spazieren können wenn sie bei einer Bestellung ihre Daten eingeben. Hinzu kommt die Gefahr, daß der Anbieter diese Daten an Dritte verkauft. Unternehmen sollten daher versuchen den Surfer offen über alle Aktivitäten in solche Richtungen zu informieren. Er sollte die Wahl treffen ob er seine Daten für diese Zwecke angeben möchte. Einen größeren Vertrauensmißbrauch im Internet könnte nämlich entscheidende Rückschläge in der Nachfrage verursachen.

5.2 Kosten/fehlende Bandbreite

Die Online-Zeit ist für die Kunden ein wichtiger Kosten-Faktor. Websites die mit aufwendigen Grafiken, Animationen usw. ausgestattet sind verschlucken Online-Zeit. Wenn der Surfer länger als ein paar Sekunden auf eine Seite warten muß, bricht er in der Regel den Ladevorgang ab.

Ein Bestellsystem, daß ein großes Sortiment anbietet, ermöglicht dem Surfer, alle Erledigungen auf einer Site durchzuführen und so Online-Gebühren zu sparen. Immaterielle Güter können zwar direkt ausgeliefert werden, aber bei größeren Datenmengen (Softwarepaketen beispielsweise) ist der Surfer besser beraten, diese im nächsten Computerladen zu kaufen als sie über die oft langsamen und überlasteten Netze zu beziehen. Die explosive Zunahme der Nutzung des Internets führt nämlich zwangsläufig zu einer Verstopfung der Netze, die sich in inakzeptablen Antwortzeiten manifestieren.

Ein Online-Anbieter sollte also versuchen die Ladezeiten seiner Seiten so gering wie nur möglich zu halten um seine Kunden nicht abzuschrecken.

5.3 Zugang

Noch ist das Internet einigen wenigen vorbehalten. In den USA sollen jetzt E-Mail-Adressen die sich aus der realen Adresse zusammensetzen, für alle Bürger eingerichtet werden. Vernetzte Computer in den Bibliotheken und Schulen sollen dann den Zugang für die nicht-Computerbesitzer ermöglichen. Hiermit soll sichergestellt werden, daß die Kluft zwischen "information rich" und "information poor" nicht weiter wächst.

Auch in Deutschland werden die Schulen und Bibliotheken als die wichtigsten Institutionen angesehen, die allen Bürgern den Zugang zu den neuen Technologien eröffnen sollen. Angesichts sinkender Haushalte und den hohen erforderlichen Investitionen ist diese Hoffnung wenig realistisch. Dennoch hat Forschungsminister Rüttgers im August 1996 1,9 Milliarden Mark für ein dreijähriges Programm zur Vernetzung deutscher Bibliotheken zur Verfügung gestellt, mit dem Ziel, jedermann vom Bildschirm aus Zugang zu den weltweiten elektronischen Informationen zu verschaffen.

Neben den Schulen und Bibliotheken schießen immer mehr "Internetcafés" aus dem Boden. Diese Cafés bieten die Nutzung eines Computers mit Internetzugang an. Die Bezahlung erfolgt pauschal zum Stundenpreis oder abhängig von der Datenmenge oder eine Kombination von beiden.

5.4 Rechtliche Aspekte

5.4.1 Vertragsrecht

Angenommen, ein Kunde aus Nigeria bestellt aus dem Online-Angebot eines deutschen Anbieters ein Produkt welches online ausgeliefert und bezahlt wird. Ab welchen Zeitpunkt besteht ein verbindlicher Vertrag? Welchen Rechtsstatus hat dieser Vertrag? Wem obliegt die Gerichtshoheit über den Vertrag?

Deutsches Recht besagt, daß ein Vertrag genau dann zustande kommt wenn zwei übereinstimmende Willenserklärungen aufeinander treffen. Willenserklärungen die auf elektronischem Wege abgegeben werden sind genauso rechtsverbindlich wie solche die mündlich oder schriftlich abgegeben werden. Das liegt daran, daß das deutsche Recht nur in ganz bestimmten Fällen eine ganz bestimmte Form vorschreibt (z.B. ist beim Kauf eines Grundstücks die Schriftform zwingend erforderlich um den Kaufvertrag rechtskräftig abzuschließen. Außerdem ist die Schriftform bei Verbraucherkreditverträgen einschließlich der Ratenkreditgeschäfte (§ 4 VerbrKrG), für Quittungen (§ 368 BGB) und für Bürgschaftserklärungen (§ 766 BGB) erforderlich). Das AGB-Gesetz (§ 2 Abs. 1) verlangt das der Verkäufer vor Vertragsabschluß auf die Einbeziehung der AGB hinweist. Der Kunde muß in zumutbarer Weise Kenntnis nehmen können von dem Inhalt der AGB. Das Lesen der langen elektronischen AGB soll aufgrund der langen Übertragungsdauer unzumutbar sein (LG Freiburg, CR 1992/93) [Dreyer 1998, 8.5.5, S. 8]. Wird bei Rahmenverträgen vorab auf die AGB hingewiesen und deren Einbeziehung vereinbart, sind die Anforderungen von § 2 AGBG erfüllt. Bei Online-Geschäften zwischen Kaufleuten verhält es sich da anders. Die AGB werden Bestandteil des Vertrages, wenn es branchenüblich ist oder im Rahmen einer laufenden Geschäftsbeziehung, so daß der Kunde damit rechnen muß den Vertrag nur auf Grundlage der AGB des Lieferanten abschließen zu können.

[Fochler 1998, S. 104] empfiehlt Online-Anbietern nach Eingang einer Kundenbestellung dem Kunden einer Annahmeerklärung zu schicken. Dieses Schreiben sollte aber nicht etwa den Kauf bestätigen. Es sollte statt dessen für das Interesse des Kunden gedankt werden und unter Hinweis auf die beiliegenden AGBs erklären daß der Anbieter das Kaufangebot gerne annimmt. Der Vertrag kommt in diesem Fall nicht dann Zustande wenn die Bestellung eingeht sondern erst mit der Annahmeerklärung des Anbieters. Da bei einer Online-Bestellung keine Unterschrift vorliegt, fehlt nämlich den Bestellungen - jedenfalls solange noch keine Infrastruktur für digitale Signaturen vorliegt - die rechtlich verbindliche Grundlage. Der Kunde kann die Annahme der Ware also ablehnen; das Risiko liegt dann beim Händler, der

die Versandkosten selbst tragen muß.

Bei der Versendung von E-Mails ist die Frage wichtig: Wann gilt die E-Mail als eingegangen? In der Rechtsprechung hat sich die Meinung gebildet, daß ein Vertragspartner, der seine E-Mail-Adresse ausdrücklich als geschäftliche Korrespondenzadresse genannt hat, so zu behandeln ist, wie derjenige, der eine Postanschrift nennt. D.h. für jeden, der seine E-Mail-Adresse im geschäftlichen Leben öffentlich (z.B. auf Visitenkarten oder Briefbögen) kommuniziert, gilt daß er sein E-Mail-Account tunlichst täglich - vorzugsweise vormittags - abfragen sollte. Eingegangene Nachrichten gehen nämlich in dem Zeitpunkt zu, in dem mit einer Leerung des Postfachs zu rechnen ist. Bei Privatleuten ist die Bestimmung dieses Zugangszeitpunktes schwierig da kein allgemeingültige Abrufzeitraum festgelegt werden kann. Übermittlungsfehler, die nachweislich auf einem Fehlverhalten seines eigenen Providers beruhen, hat der Online-Anbieter selbst zu vertreten, denn er hat diesen schließlich eigenständig ausgewählt. Er kann bestenfalls Regreßansprüche beim Provider geltend machen.

Neben der Frage des Zugangs ist noch wichtig: Welche Beweiskraft haben E-Mails? Eine Urkunde ist nach der Zivilprozeßordnung eine Gedankenäußerung, die verkörpert und deren Aussteller erkennbar ist. Digitale Dokumente erfüllen die Voraussetzung der Verkörperung nicht [Fochler 1998, S. 105]. Hier kommt das Signaturgesetz (SigG) ins Spiel. Hiernach soll ein elektronisches Dokument als beweissicher gelten, wenn die Echtheit einer dabei verwendeten elektronischen Unterschrift mit einem öffentlichen Schlüssel überprüft werden kann, der durch ein zur Zeitpunkt der Unterschrift gültiges Zertifikat einer zugelassenen Zertifizierungsinstanz bestätigt ist. Das SigG ist der umfangreichste Artikel des Informations- und Kommunikationsdienstegesetzes (IuKDG) vom Juni 1997, meist verkürzend "Multimediasgesetz" genannt. Die digitalen Signaturen des SigG basieren ausschließlich auf asymmetrischer Kryptographie: Sie arbeitet mit zwei Schlüsseln, die gemeinsam erstellt werden und mathematisch voneinander abhängig sind. Der "geheime Schlüssel" dient zur Berechnung der Signatur, der andere wird veröffentlicht und dient zur Verifikation der geleisteten Signatur. Um die digitale Signatur einer Person zuzuordnen, muß deren Name an den öffentlichen Schlüssel gebunden werden. Das erfolgt in Form eines digitalen Zertifikats, das eine vertrauenswürdige Instanz ausstellt. Das Gesetz sieht einen "Zeitstempel" vor, mit dem nachgewiesen werden kann, daß bestimmte digitale Daten zu einem bestimmten Zeitpunkt vorgelegen haben. Das SigG läßt "andere Verfahren" ausdrücklich zu, "soweit nicht digitale Signaturen nach diesem Gesetz durch Rechtsvorschrift vorgeschrieben sind". Eine SigG-konforme Signatur garantiert aber noch keinen Erfolg vor Gericht. Elektronische Dokumente unterliegen der freien Beweiswürdigung der Richter. Es ist aber zu erwarten, daß SigG-konforme Signaturen mehr Beweiswert beimessen werden als nicht-konforme. Trotzdem sollte die Zivilprozeßordnung um die Anerkennung von signierten digitalen Dokumente erweitert werden. Damit würde der Gesetzgeber auch dem hohen technischen und organisatorischen Aufwand von SigG-konformen Signaturen eine entsprechende Bedeutung beimessen [c't 16/98 (2), S. 161]. Die rechtliche Handhabung soll jedes

EU-Land für sich selbst regeln. Die einzige Vorgabe ist, daß die Anonymität als Recht des Einzelnen geachtet und "nicht ohne Notwendigkeit eingeschränkt" werden soll².

5.4.2 Datenschutzrecht

Das Gesetz über den Datenschutz bei Telediensten (Teledienstedatenschutzgesetz - TDDSG) regelt den Schutz von personenbezogenen Daten. Unter Telediensten fallen u.a. "Angebote von Waren und Dienstleistungen in elektronisch abrufbaren Datenbanken mit interaktivem Zugriff und unmittelbarer Bestellmöglichkeit" (§ 2 Abs. 5 Teledienstegesetz - TDG). Der Diensteanbieter darf personenbezogene Daten nur mit gesetzlicher Erlaubnis oder der Einwilligung des Betroffenen erheben, verarbeiten und nutzen (§ 3 Abs. 1 TDDSG). Die Bestandsdaten des Diensteanbieters beinhalten alle personenbezogene Daten die für die Begründung, inhaltliche Ausgestaltung und Änderung eines Vertragsverhältnisses erforderlich sind. Deren Verarbeitung oder Nutzung für Zwecke der Beratung, Werbung, Marktforschung oder zur bedarfsgerechten Gestaltung des Teledienstes ist nur mit der ausdrücklichen Erlaubnis des Betroffenen zulässig (§ 5 TDDSG).

Das Internet wird gerne genutzt um gerade zu diesen Zwecken Informationen über die Surfer sammeln. Der Nutzer ist aber vor der Erhebung über Art, Umfang, und Zweck der Erhebung und Nutzung seiner personenbezogenen Daten zu unterrichten (§ 8 Abs. 3 TDDSG). Er ist außerdem berechtigt, jederzeit die zu seiner Person gespeicherten Daten unentgeltlich einzusehen (§ 7 TDDSG).

5.4.3 Internationalität

Bei den zuvor besprochenen Gesetzen handelt es sich um deutsches Recht. Bei binationalen Verträgen gelten vielleicht internationale Abkommen soweit solche für die beiden Länder existieren. Wenn es keine internationale Abkommen gibt, gilt vorrangig immer das von den Parteien gewählte Recht (Art. 27 EGBGB). Wurde keine Rechtswahl getroffen, wird das Heimatrecht desjenigen Vertragspartners angewandt, der die Leistung erbringt (Art. 28 EGBGB). Als "Heimat" gilt in der Regel der Sitz des Unternehmens. Wenn aber ein deutscher Verbraucher in deutscher Sprache umworben wird, die Vertragssprache Deutsch ist und der Kunde in deutscher Währung bezahlen soll, dann ist der Sitz des Anbieters nicht maßgebend.

Deutschland gilt auch dann als Heimat wenn der Sitz dieser Firma in der Südsee liegen sollte.

5.4.4 Fernabsatz

Ein Vertrag im Fernabsatz ist jeder Vertrag der nach einer Bestellaufforderung per Drucksache oder mit Hilfe eines elektronischen Kommunikationsmediums, also z.B. per Katalog, Presseanzeige, Fax, Telefon oder eben Internet-Shop, ohne gleichzeitige körperliche Anwesenheit des Gewerbetreibenden und des Verbrauchers

abgeschlossen wird. Die Europäische Union diskutiert die entsprechenden Vorschrift derzeit. Im wesentlichen sehen die Entwürfe vor,

- daß dem Verbraucher ein Widerrufsrecht von sieben Tagen eingeräumt werden muß
- daß ihm ausführliche Informationen bereitgestellt werden müssen und
- daß er vor mißbräuchliche Praktiken geschützt werden soll.

5.5 Umsatzsteuer

Bonn plant bis Herbst dieses Jahres (1998) konkrete steuerpolitische Rahmenbedingungen für den elektronischen Handel im Internet zu schaffen. Ziel dieser Anstrengungen ist ein weltweites computergestütztes Steuereinzugssystem. Das Verfahren, bekannt unter dem Schlagwort Umsatzsteuerharmonisierung soll allen OECD³-Mitgliedstaaten erlauben, Mehrwertsteuer im ausländischen (elektronischen) Geschäftsverkehr einzubehalten. Die generelle Mehrwertsteuerpflicht endet nämlich an den nationalen Grenzen. Für die konkrete Umsetzung liegen noch keine Pläne vor, doch die Abgabe soll automatisch einbehalten und an die zuständigen Finanzämter weitergeleitet werden.

Auf seiten der deutschen Wirtschaft treffen die Steuerpläne allerdings auf breite Ablehnung. Die Anbieter von elektronischen Zahlungssystemen weigern sich bisher standhaft, solche automatischen Steuereinzugsmechanismen in ihre Software zu implementieren. Der Deutsche Industrie- und Handelstag (DIHT) erteilte dem Finanzministerium bereits eine eindeutige Absage: Das in Zahlungssysteme implementierte automatische Steuerabzugsverfahren stoße auf "gravierende steuersystematische und praktische Bedenken". Rechtlich sei eine Besteuerung des Zahlungsverkehrs nicht durchsetzbar; schließlich sei die bloße Übertragung von Geld nach geltendem EU-Umsatzsteuerrecht keine besteuerbare Leistung. Der DIHT bezeichnete die Pläne sogar als "willkürlich und umsatzsteuerlich völlig systemfremd", "rechtlich nicht haltbar" und in der Praxis "weder tauglich noch umsetzbar". Es bleibt abzuwarten, was auf Grund des geschlossenen Widerstands von den hochfliegenden Plänen am Ende des (Wahl-)Jahres noch übrig bleibt [c't 9/98 (2), S. 18].

In den USA dagegen, genauer in Kalifornien, hat der Gouverneur Pete Wilson für drei Jahre alle Internet-Geschäfte, die über Kalifornien abgewickelt werden, von der Umsatzsteuer befreit um den Internet-Handel zu fördern und Kalifornien zum wichtigsten Standort für E-Commerce zu machen [CZ 36 1998, S. 5]. In den USA werden Mehrwertsteuern nur in dem Bundesstaat einbehalten, in dem sie auch verursacht werden. Kunden in Oregon zahlen beispielsweise bei Amazon (www.amazon.com) keine Mehrwertsteuer da Amazon im Bundesstaat Washington beheimatet ist.

5.6 Zahlung

Die Online-Bezahlung ist in Deutschland noch nicht so verbreitet wie beispielsweise in den USA. Dieses Thema wird daher in Kapitel 8 zur Zukunft von E-Commerce behandelt.

5.7 Sicherheit

Die Unsicherheit von Transaktionen im Internet ist das größte Hemmniss der E-Commerce Entwicklung. Die Teilnehmer müssen darauf vertrauen können, daß ihre elektronische Transaktionen privat und unverändert bleiben. Kapitel 8 behandelt auch die Sicherheitsmechanismen die eine sichere Übertragung und Speicherung der Daten gewährleisten.

¹Siehe auch [Anhang B: Cookies](#)

²Siehe auch [Kapitel 8.5 Certification Authority](#)

³Organisation for Economic Co-operation and Development. Mitglieder sind Europa, Nord Amerika, Japan, Australien, Neuseeland, Finnland, Mexiko, die Tschechische Republik, Ungarn, Polen und Korea.





Kapitel 6: WIE WIRD E-COMMERCE GEMACHT?

6.1 Phasen einer Online-Bestellung

Im Prinzip können alle 4 Phasen der Abwicklung einer Online-Bestellung (nachfolgend vorgestellt) ohne Medienbruch im Internet erfolgen. Der Kunde wird bei seiner Suche unterstützt und kann den Kauf direkt tätigen. Der Kaufbetrag kann online bezahlt werden und bei immateriellen Gütern wie Informationen, Software oder Audiodateien beispielsweise, kann auch die Auslieferung übers Internet erfolgen. Bei einer Anbindung an die internen Datenbanken des Lieferanten kann der Verkauf sogar direkt in der Buchhaltung gebucht werden.

In der Praxis in Deutschland erfolgt der erste Medienbruch bei der Zahlung. Bei materiellen Gütern kann die Auslieferung automatisiert werden durch eine Kopplung an die Logistik des Unternehmens oder auch das Bestellwesens seines Lieferanten. Und somit erfolgt der nächste Medienbruch mit der Auslieferung der Ware.

6.1.1 Verkaufsvorbereitungsphase

Diese Phase beinhaltet alle Aktivitäten die zum Bestellangebot des Kunden führen. Der Kunde ruft die Einstiegsseite des Online-Anbieters ab. Meist findet er hier schon Links zum Produktkatalog. Der Schritt in den Produktkatalog kann mit einem Login versehen werden. Dies ist üblich, wenn nur bestimmte Kundengruppen die Produktdaten abrufen sollen (z.B. bei Bestellsystemen von Großhändlern die sich nur an Fach- oder Einzelhändler wenden). Einen Privatkunden könnte diese Registrierung beim Einstieg abschrecken, daher werden die Kundendaten oft erst zum Ende des Bestellvorgangs abgefragt. Die "Storefront" bietet in der Regel eine Übersicht der Warengruppen und optional auch Hinweise zu aktuellen Sonderangeboten. Der Kunde kann jederzeit von eine Warengruppe in die andere wechseln und dort die einzelnen Produkte einsehen. Möchte er etwas kaufen, so legt er es in den "Warenkorb". Der Warenkorb oder auch Einkaufszettel ist eine wichtige Metapher von Online-Shops. Er wird vom System geführt und der Kunde kann jederzeit den aktuellen Stand abrufen und gegebenenfalls den Warenkorb bearbeiten.

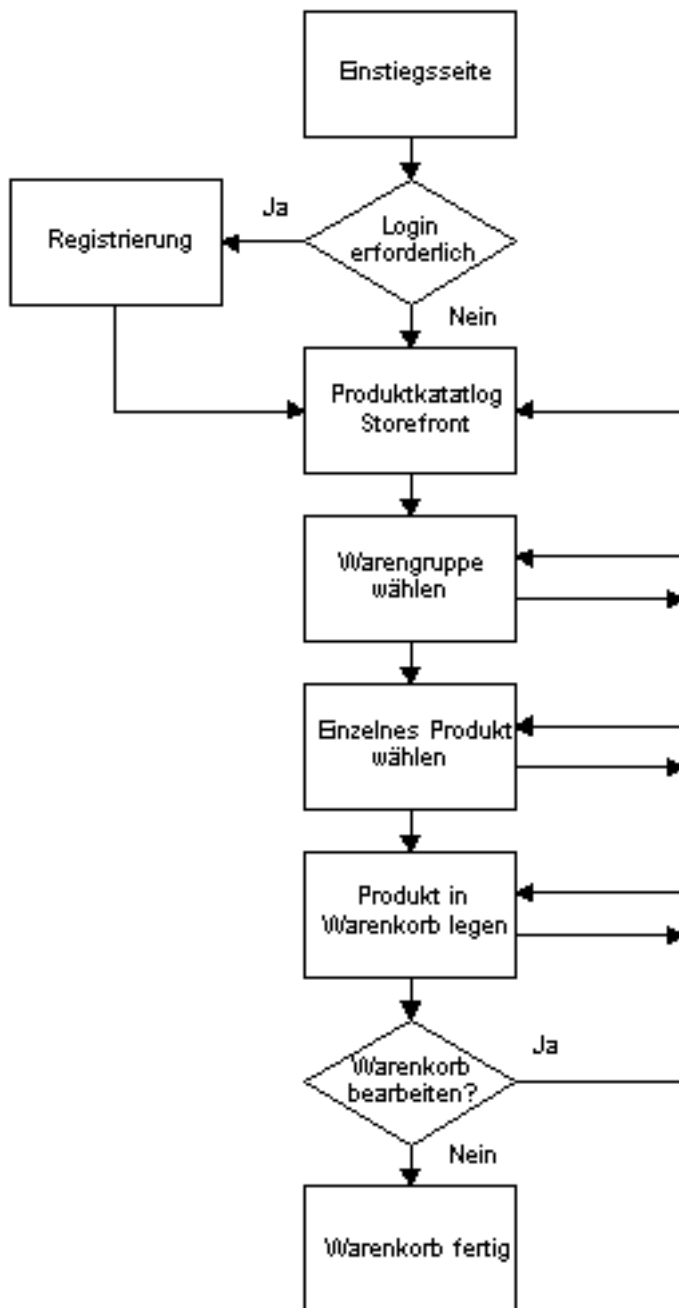


Abbildung 3: Phase 1 der Online-Bestellung

6.1.2 Bestellangebot des Kunden

In dieser Phase gibt der Kunde zu Erkennen, daß er gewillt ist die Produkte in seinem Warenkorb zu den Geschäftsbedingungen des Anbieters zu beziehen. Wenn die Registrierung nicht beim Einstieg erfolgte, dann verliert der Kunde spätestens jetzt seine Anonymität. Seine Identität und eine Lieferadresse müssen jetzt eingetragen werden. Oft kann eine Versandart und auch die Zahlungsart ausgewählt werden. Die angebotenen Zahlungsalternativen können auch kundenspezifisch zusammengestellt werden. Ein Stammkunde könnte z.B. "per Rechnung" auswählen während ein Neukunde nur die Möglichkeiten "Per Kreditkarte" oder "Per Nachnahme" angezeigt bekommt.

Ist das Bestellsystem an Kundendatenbanken angebunden, können hier auch Bonitätsprüfungen stattfinden. Denkbar ist auch die Gewährung kundenspezifischer Rabatte.

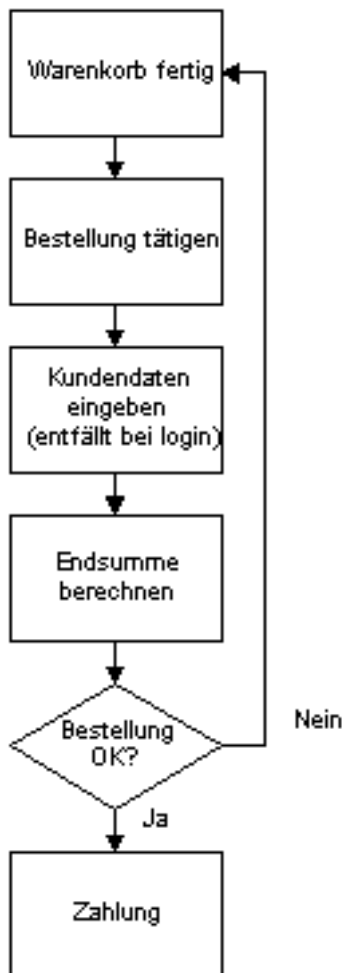


Abbildung 4: Phase 2 der Online-Bestellung

6.1.3 Zahlung und Lieferung

Bei immateriellen Gütern die online bezahlt werden können Bestellung, Zahlung und Lieferung fast zeitgleich abgewickelt werden. Im Falle von materiellen Gütern erfolgt die Lieferung in der Regel frühestens 24 Stunden später. Die Produkte können vorab online oder per Überweisung bezahlt werden. Andere Alternativen wären Lieferungen per Nachnahme oder auf Rechnung.

Die Bestellung des Kunden kann direkt in den Versand weitergeleitet werden oder eine entsprechende Bestellung bei dem Lieferanten des Anbieters auslösen. So können auch unternehmensübergreifende Prozessketten aufgebaut werden. Die Verbuchung der Zahlung, sofern online getätigt, erfolgt automatisch, wie auch die Regulierung beim Lieferanten. Da bietet es sich an, die Debitoren- und Kreditorenbuchhaltung mit einzubinden.



Abbildung 5: Phase 3 der Online-Bestellung

6.1.4 Aftersales

Alle Aktivitäten der Kundenbetreuung nach dem Kauf und der Lieferung fallen in die Phase Aftersales (nach Kauf). Hierzu gehören Support und Reklamationsabwicklung, aber auch die Versorgung mit aktuellen Informationen über neue Produkte. Für Treiber-Updates und Software-Fixes ist der Abruf über die Website des Herstellers heute schon üblich. Informationen oder Tips zu den angebotenen Produkten können hier auch oft gefunden werden. Reklamationsdaten wie auch Anfragen können mit Hilfe von HTML-Formularen aufgenommen werden und automatisch zur Verarbeitung weitergeleitet werden. Ein weitere Service wäre es, wenn der Kunde seine bisher getätigten Bestellungen abrufen oder seine offene Posten anzeigen lassen kann.

6.2 Vorüberlegungen

Vor dem Schritt ins Internet, müssen folgende Fragen geklärt werden:

- **Sind die Produkte internetvertriebsfähig?**
Grob gesagt ist alles für den Online-Vertrieb geeignet was auch über einen Versandhandel vertrieben werden kann¹.
- **Welche Erwartungen werden an die Website gestellt?**

Das können sein: Umsatzsteigerungen, Prestige, Kundennähe usw.

- **Reichen die vorhandenen Kapazitäten aus?**

Reichen die vorhandenen Kapazitäten aus um zusätzliche Aufträge flott zu bearbeiten? Wie paßt es in die Geschäftsprozesse? Sind Kapazitäten zur späteren Pflege der Webseiten vorhanden?

- **Sind die Mitarbeiter den Anforderungen gewachsen?**

Mit der neuen Internetpräsenz sind auch die Mitarbeiter gefordert Anfragen per E-Mail zu bearbeiten und beantworten.

- **Wie kann der Erfolg oder Mißerfolg gemessen werden?**

Die folgenden Meßgrößen können zur Erfolgsmessung auf seiten der Website genutzt werden: Page Clicks: die Anzahl der Aufrufe einer HTML-Seite wird hier dokumentiert. Page Views: dieser Wert zählt alle ohne Abbruch erfolgten Aufrufe einer bestimmten HTML-Seite. Die Logfile-Analyse ist eine Alternative die festhält wer die Seiten abgerufen hat. Allerdings speichert diese nicht die Adressen der Surfer sondern die der Hostrechner über den der Zugang erfolgte. Inzwischen werden auch Programme für Webserver angeboten, die die Zahl der Nutzer pro Zeiteinheit messen.

- **Wer gehört zur Zielgruppe?**

Endverbraucher, Fachhändler, Großhändler usw.

- **Verfügt die Zielgruppe im Allgemeinen über einen Internetzugang?**

Die Zielgruppe kann natürlich nicht erreicht werden wenn diese nicht über einen Internetzugang verfügt oder diesen nicht nutzt. Kundenumfragen starten und ggfs. Aufklärungsarbeit leisten.

- **Welche Inhalte?**

Welche Informationen sollen dargestellt werden? Ist die Information aktuell? Ist dieser Inhalt auch interessant für den Surfer? Was heißt eigentlich „interessant“? informativ - sowohl für den schnellen Überblick als auch für tiefen Einblick interaktiv - je nach den individuellen Informationsbedürfnissen attraktiv - angenehme Optik, anregende Ansprache, akzeptable Aufrufzeiten vielseitig - mit neuen Erkenntnissen auch bei Wiedereinsteigern transparent - Übersicht, ohne den Überblick im Info-Dschungel zu verlieren spannend - Thrill, Fun, Entertainment. Schließlich soll es auch unterhaltend sein.

Sind die Vorüberlegungen abgeschlossen, ist die Implementierung mit geeigneten Tools unter Berücksichtigung des geplanten Bestellablaufes und der Datenquelle dran. Das Design folgt als nächster Arbeitsschritt. Die Werbung ist ein äußerst wichtiger Abschnitt für den Erfolg der neuen Internetpräsenz. Und die Pflege der Website kommt zuletzt und ist eine kontinuierliche Aufgabe.

6.3 Wahl des Providers

Ein Internet Service Provider (ISP) ist ein Dienstleistungsunternehmen, das Internet-Zugänge für Privat- und Geschäftskunden anbietet. Ein Provider verfügt über eine Verbindung zu einem Internet-Backbone. Internet-Backbones sind Hochgeschwindigkeitsnetze, die das Rückgrat des Internets bilden. Die Provider

erhalten über Standleitungen² Anschluß an das jeweilige Backbone-Netz. Der Kunde kann sich dann durch das Einwählen beim Provider mit dem Internet verbinden. Außer den Internet-Zugängen und verwandte Dienste wie E-Mail-Adressen stellen viele Provider auch Ressourcen für die Ablage (Speicherplatz auf dem Webserver) und gegebenenfalls Erstellung von Webseiten (Mitarbeiter Know-how) zur Verfügung.

Einige wichtige Kriterien bei der Wahl eines geeigneten Providers sind:

- **Netzzuverlässigkeit:**
Das Netz sollte möglichst störungsfrei laufen.
- **Sicherheitskonzepte:**
Der Provider sollte geeignete Maßnahmen zur Absicherung des Datenverkehrs und des Datenbestandes einsetzen³.
- **Netzwerkdurchsatz:**
Ein hoher Netzdurchsatz ist für alle die die Website abrufen angenehm, seien es die Kunden oder auch die eigenen Mitarbeiter.
- **Erfahrung/Referenzen:**
Über die schon vorhandene Kunden können Informationen zu den anderen Kriterien (wie Netzdurchsatz oder Netzzuverlässigkeit) eingeholt werden.
- **Regionale Nähe:**
Der gewählte Provider sollte möglichst im Ortstarifnetz des Anbieters angesiedelt sein oder einen Zugang zum Ortstarif anbieten.
- **Kosten:**
Die Preisgestaltung der Provider ist sehr unterschiedlich. Die Abrechnung für die Ablage kann beispielsweise nach benutztem Speicherplatz oder nach Anzahl der HTML-Seiten erfolgen. Deshalb sollten Kostenvoranschläge über die gewünschten Leistungen eingeholt werden von den in Frage kommenden Providern. Jeder erstellt einen Kostenvoranschlag nach seinen Preislisten und die Gesamtsumme ist dann vergleichbar.
- **Service/Hotline**
- **Zukunftspläne:**
Die Offenheit des Providers gegenüber Neuerungen ist ein sehr wichtiges Kriterium. Da das Internet sich ständig weiterentwickelt, sollte auch der Provider die eingesetzten Verfahren durch erprobte Weiterentwicklungen ersetzen.

6.4 Datenquelle

Ein Bestellsystem im Internet wird benutzt um die Produkte einer Firma zum Verkauf anzubieten. Die Informationen zu den Produkten (eine Beschreibung, der Preis usw.) müssen aufbereitet und zur Verfügung gestellt werden. Diese Informationen stellen die Datenquelle dar. Die Datenquelle kann alles von einer "comma-separated-values" Textdatei für kleinere Angebote bis einer relationalen Datenbank sein. Die Produktseiten können auch als statische HTML-Seiten abgelegt werden. Die

Verwaltung solcher Seiten ist aber recht aufwendig und lohnt sich wirklich nur dann wenn der Umfang der Produkte nicht zu groß ist. Der Vorteil von Datenbanken liegt darin, daß die Produktinformationen zur Laufzeit in HTML-Schablonen aufgenommen und dargestellt werden können und daher immer aktuell sind. Außerdem erfolgt die Verwaltung einfach über die Datenbankwerkzeuge.

Die Auswahl der Datenquelle hängt erstens davon ab, ob das Bestellsystem an die firmeninterne Produktdatenbank angeschlossen werden soll/kann. Dies hat den Vorteil das im Datenfluß kein Bruch besteht und immer aktuelle Daten geliefert werden. Ist dies der Fall, so ist die zweite Frage schon fast beantwortet, und zwar ob das Bestellsystem auf einem firmeninternen Server betrieben wird oder auf einem Server des Providers. Ein eigener Webserver hat den Vorteil, daß auch der Zugriff auf vorhandene Kunden- und Rechnungsdaten denkbar wäre (z.B. um offene Posten des Kunden für diesen abrufbar zu machen usw.). Ein weitere Vorteil ist der Wegfall von Medienbrüchen zwischen Quelle und Darstellung. Der Nachteil ist, daß die Firma selber auf ausreichende Sicherheit achten und für geschultes Personal sorgen muß. Angriffe von außen können mit Hilfe einer Firewall abgewehrt werden. Zusätzlich sollten kritische Kundendaten nur über Paßwörter zugänglich sein. Wenn das Bestellsystem auf dem Server des Providers laufen soll, muß der Kunde in der Regel das vom Provider eingesetzte Betriebs- und Datenbanksystem benutzen.

Als weiteres Kriterium zählt auch der Umfang den die Produktdaten haben und wie oft diese aktualisiert werden. Für ein kleines, starres Sortiment ist es nicht notwendig bei jedem Aufruf eine Datenbanken auszulesen. Hier wäre es denkbar, die Produktdaten direkt in die HTML-Seiten zu schreiben.

6.5 Implementierung

Die Implementierung hängt zum Teil von der gewählten Datenquelle ab. Neben der Erstellung ist auch die spätere Pflege der Seiten ein zu beachtender Aspekt. Im folgenden werden fünf mögliche Methoden zur Implementierung von Bestellsystemen vorgestellt.

6.5.1 CGI

Mit CGI (Common Gateway Interface) kann ein Browser auf den anbietenden⁴ Server Scripts auszuführen (beispielsweise um Formulareingaben aus HTML-Dateien zu verarbeiten oder auf dem Server Daten zu speichern und dort gespeicherte Daten auslesen). Die sogenannte CGI-Schnittstelle steht zur Verfügung, wenn ein WWW-Server installiert ist der CGI unterstützt. Die CGI-Schnittstelle besteht aus:

- einem bestimmten Verzeichnis auf dem Server, das CGI-Programme enthalten darf. Meist erhält dieses Verzeichnis den Namen cgi-bin oder cgi-local.
- einer Reihe von Daten, die der Server speichert und die ein CGI-Script auslesen kann (und zum Teil auslesen muß), um Daten verarbeiten zu können.

Diese Daten speichert der Server in sogenannten CGI-Umgebungsvariablen. Mögliche Inhalte solcher Variablen sind Browsertyp oder Eingabedaten eines Formulars.

CGI Skripts können mit vielerlei Programmiersprachen geschrieben werden. Perl ist jedoch die meistbenutzte Programmiersprache für CGI-Skripts. U.a. weil Perl sehr mächtige Funktionen besitzt (z.B. für Zeichenkettenoperationen oder für das Lesen und Schreiben von Daten) und weil der Perl-Interpreter, der zum Ausführen eines Perl-Skripts erforderlich ist, für fast alle Betriebssysteme als Freeware verfügbar und auf fast allen Servern installiert ist [Münz 1997].

CGI Skripts können entweder von HTML-Seiten aufgerufen werden (z.B. wenn ein Formular zur Prüfung an den Server geschickt wird) oder selber HTML Seiten generieren (z.B. um den Empfang einer eingehenden Bestellung zu bestätigen).

Die Website <http://www.itm.com/cgicollection/> ist eine gute Anlaufstelle für fertigen Quellcode, Einführungen, Bücher, Newsgroups, FAQs usw.

In dem folgendem Beispiel können die Felder "UserName" und "Text" in einem Formular einer HTML-Seite ausgefüllt werden.

```
<HTML>
<HEAD>
<TITLE> Kommentarseite </TITLE>
</HEAD>

<BODY>
Ihr Kommentar <P>

<FORM ACTION="/cgi-bin/comments.pl" METHOD=post>
Name: <INPUT SIZE=40 NAME="UserName">
Text: <TEXTAREA ROWS=5 COLS=70 NAME="Text"> </TEXTAREA>
<INPUT TYPE=submit VALUE="Absenden">
</FORM>

</BODY>
</HTML>
```

Tabelle 4: Beispieldatei "form.htm"

Ein Mausklick des Buttons "Absenden" führt dann das in Perl geschriebene Programm "comments.pl" aus. Dieses Programm gibt die Eingaben des Nutzers auf einer neuen HTML-Seite wieder aus.

```
#!/usr/bin/perl

read(STDIN, $Daten, $ENV{'CONTENT_LENGTH'});
print 'Content-type: text/html\n\n';
print '<HTML> <HEAD> <TITLE> CGI-Feedback </TITLE>
</HEAD>\n';
print '<BODY> <H1> CGI-Feedback vom Programm <I>
comments.pl </I> </H1>\n';
@Formularfelder = split(/&/, $Daten);
foreach $Feld (@Formularfelder)
{
($name, $value) = split(/=/, $Feld);
$value =~ tr/+// /;
$value =~ s/%([a-fA-F0-9][a-fA-F0-9])/pack("C",
hex($1))/eg;
$value =~ s/ <!--(.\n)*-- > //g;
$Formular{$name} = $name;
$Formular{$value} = $value;
print $Formular{$name} = $Formular{$value}, '<BR>\n';
}
print '

\n';
```

Tabelle 5: Beispieldatei "comments.pl"

6.5.2 Javascript

Javascript ist eine Skriptsprache die von Sun Microsystems und Netscape Communications eingeführt wurde. Javascript erweitert die Fähigkeiten einer HTML-Seite. Es ermöglicht Interaktivität (Feedback, Formulare usw.) und Dynamik (Animationen usw.).

Es gibt zwei Typen von Javascript-Programmen: nämlich Client-side Javascript und Server-side Javascript mit denen Anwendungen erstellt werden, die im Browser bzw. auf dem Server laufen. Client-side Javascript wird direkt im HTML-Code eingebettet oder als separate Datei inkludiert. Ein Browser liest den HTML-Code sequentiell und stellt ihn dar. Javascript Code wird direkt vom Browser interpretiert. Client-side Javascript kann nicht auf fremde Dateien zugreifen. Als "fremd" zählen die Dateien auf der Festplatte des Surfers und die auf dem anbietenden Server. Allerdings kann Javascript mit Hilfe von Liveconnect mit Java Anwendungen und Applets kommunizieren und so indirekt auf den Host (z.B. auf Datenbanken) zugreifen.

Server-side Javascript wird ebenfalls direkt im HTML Code eingebettet oder inkludiert. Allerdings wird die HTML Datei zusammen mit dem Javascript Code in

ausführbaren Bytecode kompiliert. Die Runtime engine des Web Servers erstellt dann zur Laufzeit⁵ die HTML-Seite und führt den Javascript Code aus. Das Session Management Service von Server-side Javascript enthält Objekte mit denen Daten persistent gespeichert werden können (zum Beispiel für den Einsatz von Zählern oder zur Erstellung von Statistiken). Der LiveWire Database Service von Server-side JavaScript stellt Objekte, die als Schnittstelle zu SQL-basierten Datenbanken dienen, zur Verfügung [Netscape 1998].

Javascript hat gegenüber CGI den Vorteil, daß der Code direkt in der Seite eingebettet ist und somit alles auf der Client-Seite ausgeführt wird. Ein CGI Skript hat nämlich den folgenden Ablauf: Daten aus einer HTML Seite werden übers Netz zum Server geschickt (z.B. Eingabedaten eines Formulars). Das CGI auf dem Server bearbeitet die Daten (z.B. Prüfung der Eingabedaten). Die Ergebnisse werden dann wieder übers Netz zurück zum Browser geschickt. Mit Javascript werden der Server und das Netz entlastet.

Die aktuelle Javascript Version ist 1.2 (Stand 07/98).

Die Webadresse: <http://www.infohiway.com/javascript/indexf.htm> bietet "Cut'n'Paste" JavaScript an. Das heißt, der Quellcode für verschiedene Funktionen kann direkt aus den Seiten heraus kopiert und in eigene Webseiten eingebunden werden.

Der folgende Beispielcode fragt Browsertyp und -version ab und leitet dann auf die entsprechende Seite. Die Funktion "choose" wird zwischen den <SCRIPT> Tags im <HEAD> Bereich eingeschlossen. Im <BODY>-Teil löst ein Klick auf das Wort: Weiter? die Funktion "choose" aus.

```
<HTML>
<HEAD>
<TITLE>Browserabfrage</TITLE>

<SCRIPT LANGUAGE="JavaScript">
<!--

function choose(){
var browser = navigator.appName;
var version = parseInt(navigator.appVersion);

if (browser == "Netscape" || "Microsoft Internet
Explorer"){
if (version >= 3)
parent.location.href="vers3.htm";
else
```

```

parent.main.location.href="vers2.htm";
}
else
parent.main.location.href="vers1.htm";
}

<!-- end script -->
</SCRIPT>

</HEAD>
<BODY>

<A HREF="javascript:choose();" >Weiter?</A>
</BODY>
</HTML>

```

Tabelle 6: Beispieldatei "check.htm"

6.5.3 Java

Java wurde von der Firma Sun Microsystems im Rahmen eines Software-Forschungsprojektes für elektronische Haushaltgeräte wie Fernseher, Videorecorder, Toaster u.Ä. entwickelt. Das Ziel war es, eine Sprache zu schaffen, die klein und schnell ist und die leicht auf die verschiedensten Hardwareplattformen portiert werden kann [Doberenz 1998, S. 31].

Das Ergebnis ist eine Sprache die streng objektorientiert ist, Multithreading unterstützt, sehr stabil läuft und plattformunabhängig ist. Der Quellcode wird vom Java-Compiler in einen binären Bytecode kompiliert. Dieser plattformunabhängiger Bytecode kann auf einer beliebiger Hardware von einem Java-Interpreter ausgeführt werden.

Es gibt zwei Typen von Programmen die man mit Java entwickeln kann: Applets und Anwendungen. Applets werden als "class"-Dateien innerhalb einer HTML-Seite eingebettet. Der Quellcode wird zu einer ".class" Datei kompiliert und die Java Virtual Machine eines Java-fähigen Browsers interpretiert das Applet zur Laufzeit. Aus Sicherheitsgründen kann ein Applet nicht auf die Dateien des Surfers zugreifen oder auf dessen Rechner eine Anwendung starten. Ein Applet kann allerdings mit anderen Applets sowie mit Anwendungen auf dem Hostrechner kommunizieren. Java Anwendungen sind stand-alone Programme. Der Quellcode wird ebenfalls zu einer ".class" Datei kompiliert. Der Java Interpreter führt dann zur Laufzeit das Programm aus. Client/Server Programme können mit einer Kopplung von Applets auf der Client-Seite und Anwendungen auf der Server-Seite realisiert werden.

Das JDK ist die Java Entwicklungsumgebung von Sun Microsystems. Es enthält neben dem Compiler, dem Interpreter, dem Debugger und dem Appletviewer noch

die grundlegenden Java-Klassen sowie zusätzliche Klassen wie die zur Internetprotokoll-Unterstützung.

Die aktuelle Version des JDK ist 1.1.6. Die Version 1.2 ist als Beta verfügbar (Stand 07/98).

Unter <http://java.sun.com:80/docs/books/tutorial/index.html> ist eine sehr ausführliche Java-Schulung zu finden. Und <http://www.javaworld.com/> bietet kostenlosen Quellcode für die verschiedensten Applets an.

Um ein Applet zu implementieren, sind zwei Dateien notwendig: eine HTML-Datei die das Applet aufruft und eine ".java"-Datei die zu einer ".class"-Datei kompiliert wird. Das folgende Beispiel gibt einen formatierten Text im Browser aus.

```
<HTML>
<HEAD>
<TITLE>Test</TITLE>
</HEAD>

<BODY>

Dies ist ein test<P>

<APPLET CODE="Test.class" WIDTH=1000 HEIGHT=200>
</APPLET>

</BODY>
</HTML>
```

Tabelle 7: Beispieldatei "test.htm"

Die Ausgabe über System.out.Print kann nur über die Java-Konsole angesehen werden oder alternativ über den Appletviewer von Sun. In dem Browser wird die Funktion "drawString" ausgeführt (und zwar formatiert nach den Angaben der "init"-Methode).

```

import java.applet.Applet;
import java.awt.*;

public class Test extends Applet {

    public void init() {
        resize(1000,200);
        setBackground(Color.blue);
        setForeground(Color.white);
        setFont(new Font("TimesRoman", Font.PLAIN, 24));
    }

    public void paint(Graphics g) {
        g.drawString("Dies ist die Ausgabe des Java Applets",
        10, 25);
    }

    public void start() {
        System.out.println("start test");
    }
}

```

Tabelle 8: Beispieldatei "Test.java"

6.5.4 SQL-Gateways

SQL-Gateways sind Schnittstellen zwischen HTML-Seiten und relationale Datenbanken. Das Gateway erweitert den Sprachumfang der HTML-Befehle um neue datenbankbezogene Befehle. Werden die - mit dem erweiterten Sprachumfang programmierten - Seiten abgerufen, so gelangt die Anfrage an den anbietenden Server. Dieser leitet die Anfragen an das SQL-Gateway weiter. Das Gateway interpretiert die Anfragen, übergibt sie an das Datenbanksystem und erhält von dort die Ergebnismenge zurück. Die Ergebnismenge wird nun so umgeformt, daß eine Darstellung in HTML möglich ist. Das Ergebnis ist dann reiner HTML-Text. Der Vorteil dieser Lösung besteht darin, daß alle zu einer HTML-Seite gehörenden Informationen - statische und dynamische - gemeinsam in einer Datei abgelegt und gepflegt werden können, statt sie getrennt zu verwalten.

Das Zusammenfassen von WWW- und Datenbankserver zu einem einzigen Softwaresystem stellt die höchste Stufe der Integration dar. Vorteile sind die Verwendung eines einzigen Systems sowohl zur Verwaltung, Darstellung und Bearbeitung interner als auch externer Informationen. Die Integration kann soweit gehen, daß die einzelnen HTML-Seiten ebenfalls in der Datenbank abgelegt und dort gepflegt werden können. Beispiele solcher Werkzeuge sind DB2WWW von IBM, das DB2 und andere Datenbanken über DataJoiner unterstützt, Cold Fusion von Allaire, das Datenbanken mit der ODBC Schnittstelle unterstützt und Oracle WebServer von

Oracle, das die Datenbank Oracle 7 unterstützt [Kracke 1996, Teil 4/9.6 S. 3].

<http://www.developer.com/> ist eine Website die Informationen (Tutorials, Quellcode, FAQs usw.) zu allen vorgenannten Methoden bietet und sehr viel mehr. Sie ist eine exzellente Informationsquelle für Internet-Programmierer. Eine sehr gute deutschsprachige Seite ist <http://www.teamone.de/selfhtml/>. Sie bietet u.a. ausführliche Informationen zu HTML und JavaScript. Die Website <http://www.alleykatt.com/coders/> enthält eine große Linksammlung zu vielen andere Websites die sich mit der Web-Programmierung beschäftigen.

6.5.5 Shop-Systeme

Shop-Systeme enthalten Demo-Shops, die sich auf die Bedürfnisse der Firma anpassen lassen. Es gibt zwei Typen: ein Shop-System mit dem eine Firma ihren Online-Laden aufziehen kann und das Mall-System, das eher an Providern gerichtet ist mit der Idee, daß sie ein Einkaufszentrum aufbauen und darin einzelne Läden einrichten. Zu den elementaren Funktionen eines Shop-Systems gehört es, aktuelle Produktdaten aus einer Produktdatenbank zu lesen und diese in eine vorbereitete Katalogseite (Template) einzusetzen. Weiter sollte das System einen Warenkorb verwalten und eventuelle Bestellungen des Kunden entgegennehmen können.

Viele Shop-Systeme bieten darüber hinaus weitere Funktionen. So kann der Kunde z.B. jederzeit den Auftragsstatus einer Bestellung abfragen oder zurückliegende Einkäufe aufrufen. Eine Auftragsbestätigung wird nach getätigter Bestellung automatisch per E-Mail verschickt. Auf Seiten der Anbieter ist die Verwaltung der Kundendaten eine weitere vorhandene Funktion. Es können außerdem zeitlich begrenzte Sonderangebote konfiguriert werden sowie ein automatisches Anbieten von ergänzenden Produkten. Verschiedene statistische Auswertungen werden unterstützt. Die Administration der Systeme erfolgt in der Regel per Browser über das lokale Netz. Üblich ist die Unterstützung von Datenbanken mit ODBC-Schnittstellen [Wasmeier 1997, S. 226].

ICat Commerce Online von iCat Europe Central (<http://www.icat.co.uk>) ist eine komplette Lösung für Einsteiger, die jedoch alle notwendigen Funktionen für den Online-Verkauf bietet. Intershop Online von der Jenaer Intershop GmbH (<http://www.intershop.de>) ist ein weiteres Beispiel für ein Shop-System. Sonstige sind Net.Commerce Suite von IBM, der Domino.Merchant von Lotus und der Microsoft Commerce Server (jetzt Bestandteil von Site Server).

Welche der vorgestellten Methoden die Beste ist, kann nicht so einfach bestimmt werden. Fertige E-Commerce-Lösungen wie die Shop-Systeme haben die Vorteile der geringeren Personalbindung und der vorhandenen Dokumentation. Erforderliche Weiterentwicklungen aufgrund von Mehrwertsteueränderungen oder der Einführung des Euros beispielsweise, können schneller und günstiger implementiert werden. Bei den Eigenentwicklungen hat der Online-Anbieter mehr Einfluß auf die Funktionalität

und kann so die Paßbarkeit zu seinem Unternehmen gewährleisten.

Welche der Lösungen zu präferieren ist, hängt vom Umfang der gewünschten Website Funktionalitäten ab. Die Anbindung an eine relationale Datenbank ist mit einem SQL-Gateway relativ leicht zu implementieren. Mit Java ist dies zwar auch möglich, allerdings erst für die Browser der vierten Generation komfortabel zu implementieren. Für die Einbindung und Prüfung von Feedback- oder Bestellformularen (ohne Produktkatalog) reichen CGI-Skripts oder JavaScript aus.

Es muß also von Fall-zu-Fall entscheiden werden, wie das E-Commerce-System implementiert werden soll.

6.6 Design

Der erste Eindruck ist das entscheidende Kriterium für den Erfolg einer Website. Das Aussehen der Site sollte die Corporate Identity der Firma unterstreichen. Die Qualität der Produkte sollte sich in der Qualität der Site widerspiegeln. Das erweckt das Vertrauen der Kunden.

Sehr wichtig ist eine klar erkennbare Navigation. Der Benutzer sollte intuitiv seinen Weg zu den Informationen finden die er sucht. Die Website sollte in der Hierarchie vom Allgemeinen zum Besonderen absteigen. D.h. von den allgemeinen Informationen der Startseite zu den detaillierteren Subseiten. Der Kern der Site, das Produkt- und Leistungsangebot, sollte klar im Vordergrund stehen. Wenn die Website sehr komplex ist, sollte eine Sitemap erstellt werden. Die Sitemap entspricht im groben ein Stichwortverzeichnis in dem jedes Stichwort zu der entsprechenden Seite führt.

Einen auf Papier vorliegenden Produktkatalog eins-zu-eins fürs Internet zu übernehmen ist nicht sinnvoll, da das Medium Internet dann nicht vollständig ausgenutzt wird. Außerdem verschwendet der Surfer kostbare Online-Zeit damit, einen Katalog durchzublättern den er in der Regel umsonst zugeschickt bekommen könnte. Die Ladezeiten sollten so kurz wie nur möglich gehalten werden.

Weiter unabdingbar ist die Angabe von Kontaktmöglichkeiten. Viele Anwender benutzen das Web als Adreßbuch um schnell eine E-Mail-Adresse, eine Telefonnummer oder den entsprechenden Ansprechpartner zu finden. Diese Angaben sollten möglichst auf oberster Ebene angezeigt werden.

Wenn neue Gestaltungstechniken wie Flash von Macromedia benutzt werden um die Site optisch aufzupeppen und interessanter zu machen, sollte dies auf der Startseite vermerkt sein. Zusätzlich sollte für Surfer mit älteren Browser ein Link auf die Downloadseite des Plugin-Herstellers führen sowie ein Link auf eine Seite die ohne die neuen Techniken gestaltet wurde.

Für Online-Anbieter die auch ausländische Kunden anwerben möchten, sollten HTML-Seiten in den entsprechenden Sprachen zur Verfügung gestellt werden.

6.7 Qualitätssicherung

- **Linktest:**
Die Links sollten vor der Online-Premiere überprüft werden. Links die ins Nirvana führen verärgern die Kunden nur.
- **Browsertest:**
Die Website sollte auf allen Browsern dargestellt werden. Ist dies nicht der Fall sollte darauf hingewiesen werden und ggf. auf eine Downloadsite verwiesen werden von der der Nutzer die entsprechende Browserversion beziehen kann.
- **Text-only:**
Versierte Surfer schalten oft die Grafiken aus, um Ladezeiten zu reduzieren. Eine Website sollte auch ohne Grafiken navigierbar sein.

6.8 Werbung (Site Promotion)

Damit eine Website auch abgerufen wird, müssen die vorhanden und die potentiellen Kunden informiert werden. Wenn niemand die Adresse kennt, wird auch niemand die Website besuchen. Wenn der Firmennamen nicht zu lang ist und die Domäne nicht schon vergeben, sollte die Website die Adresse `www.firmenname.de` haben. Sollte der Produktname einen höheren Bekanntheitsgrad haben als der Firmenname sollte die Domäne `www.produktname.de` gewählt werden. Bis zum 1. Februar 1997 konnte jeder beim Deutschen Network Information Center (DENIC, zuständig für die Registrierung von DE-Domänen) einen Domännamen für sich reservieren lassen. Die Kosten hierfür von 160 Mark zuzüglich Umsatzsteuer waren relativ günstig. Die Domäne war dann für ein Jahr geschützt. Als dann einige Provider populäre Namen reservierten um sie teuer weiter zu verkaufen, hat die DENIC die Reservierungspraxis geändert. Wer heute eine Domäne reserviert, muß diese auch im Internet nutzen - genauer gesagt, zur Nutzung auf einen Server delegieren, was mit deutlich höheren Kosten verbunden ist.

6.8.1 Rundschreiben

Eine Firma sollte mit einem Rundschreiben und Vermerken (z.B. Stempel oder Aufkleber) auf der ausgehenden Post, ihre Geschäftspartner auf die neue Website aufmerksam machen. Die URL und die E-Mail Adresse müssen überall stehen wo auch die Anschrift des Unternehmens steht. Also auf dem Briefkopf, in Printanzeigen usw.

6.8.2 Service

Ganz besonders jetzt am Anfang des Online-Zeitalters sollte jeder Kunde wie ein König behandelt werden, da sehr viel über Mundpropaganda erreicht wird und eine Online-Bestellung immer noch etwas seltenes ist, über das man gerne spricht. Die Loyalität der Kunden kann gewonnen werden indem deren E-Mails mit Bestellungen, Anfragen und Kritik grundsätzlich innerhalb von 24 Stunden beantworten werden. Der Kunde sollte das Gefühl bekommen, daß der Lieferant sich für ihn und seine Probleme interessiert. Der Vorteil der geographischen Nähe zum Kunden ist nämlich im Internet irrelevant geworden. Es ist erst der besondere Service eines Online-Anbieters, der ihn hervorhebt und den Kunden zum Kauf animiert. Dieser besondere Service kann z.B. ein Newsletter sein, mit Neuigkeiten aus der Branche oder mit Nachrichten über neue Entwicklungen etc.

6.8.3 Aktionen

Die Kunden sollten mit Sonderangeboten oder anderen Aktionen angeregt werden online zu bestellen. Die Firma Macrotron Distributions GmbH, ein Großhändler und Hersteller von Hard- und Software in München, belohnte alle Online-Bestellungen die in den ersten zwei Monaten der Online-Präsenz eingingen mit kostenloser Lieferung [Macrotron 1998]. Weitere mögliche Aktionen sind: Gewinnspiele oder Rabatte.

6.8.4 Suchmaschinen

Suchmaschinen sind häufig die erste Anlaufstelle des Surfers auf dem Weg zur gesuchten Website. Der Name der Firma und die Bezeichnung der Produkte sollten deshalb in den bekanntesten Suchmaschinen (z.B. [Altavista](#)) und Web Directories (z.B. [Yahoo](#)) eingetragen werden. Firmenverzeichnisse wie www.industrienet.de oder www.wlwonline.de (Wer liefert was) sollten ebenfalls genutzt werden. Auch Online-Branchenbücher wie www.web.de sind wichtige Einstiegsseiten für einen Surfer. Gibt es für die Branche zusätzlich noch andere Suchdienste, sollten auch hier die entsprechenden Einträge gemacht werden.

6.9 Pflege

Das Internet ist ein schnelles Medium. Deshalb sollten die Inhalte von Websites regelmäßig aktualisiert bzw. erneuert werden. Der Nutzer einer Site besucht sie ein weiteres Mal weil:

- Er noch nicht alle Inhalte kennt. Entweder weil sie so umfangreich ist (z.B. Online-Lexikon) oder weil ein häufiges Update stattfindet. Ein EDV-Händler z.B. verkauft Ware für die häufig Tagespreise gelten, die bis zum Druck und Versenden von Katalogen veraltet sind.
- Es sich für ihn lohnt, die Site nochmal aufzurufen (z.B. Bestellsystem) [Werner 1997, S. 76].

Bezüglich der Aktualität der WWW-Angebote wurde bei der Untersuchung [Kurbel 1997] gefragt, in welchen Zeitabständen die Unternehmen ihre Seiten aktualisieren. Etwa 42 % bringen die Informationen mindestens alle zwei Wochen auf den neuesten Stand (10 % sogar täglich). Circa ein Viertel hält eine monatliche Aktualisierung für ausreichend.

Die folgenden Punkte sollte ein Webmaster in Zusammenarbeit mit der Werbeabteilung durchführen um für die Aktualität, Gültigkeit und Attraktivität zu sorgen:

- **Kundenumfragen:**

Kundenumfragen zu der Website zeigen auf, welche Bereiche gelungen sind und welche eben nicht. Solche Kritik sollte in die Neugestaltung einfließen. Ein positiver Nebeneffekt: der Kunde fühlt sich ernst genommen. Außerdem kann man mit weniger finanziellem und personellem Aufwand einen weiter gestreuten Personenkreis erreichen als konventionell per Post. Auch die Auswertung ist leichter, da die Daten schon digital vorliegen.

- **News:**

Artikel aus der Presse oder das Bekanntgeben neue Produkte sind Neuigkeiten, die regelmäßig aktualisiert werden können. Auch sehr wichtig und interessant sind die Ergebnisse angebotener Produkte aus Tests unabhängiger Stellen, Umsatzsteigerungen mit verbundenen Einstellungen sowie Anstrengungen in Richtung Umweltschutz.

- **Statistiken:**

Anhand von Webstatistiken kann festgestellt werden, welche Seiten häufig aufgerufen werden und ob das Interesse an bestimmten Seiten nachläßt. Diese Ergebnisse sollten als Anstoß zum Re-Design gelten.

- **Kundenanfragen:**

Diese müßten so schnell wie möglich erledigt werden. Vorab sollte geklärt werden ob die Mails zentral an info@firma.de oder direkt an die zuständigen Sachbearbeiter geschickt werden sollen. Die zentrale Verwaltung hat den Vorteil, daß Auswertungen über die Anzahl der Mails, den Inhalt etc. ausgeführt werden können. Auf der anderen Seite, hat das Angeben von spezifischen Ansprechpartners, eine persönlichere Note.

- **FAQs:**

Ein weiterer Service ist es, die E-Mails der Kunden zu einer FAQ Liste auszuarbeiten. Diese Liste beinhaltet Fragen die häufig von Kunden gestellt wurden und die dazugehörigen Antworten.

6.10 Wichtige Funktionen eines Bestellsystems

Die folgenden Funktionen sind auszugsweise von [Fochler 1998, S. 210 f] als Wunschliste an Merchant-Entwickler⁶ zusammengestellt worden. Sie können auch als Anforderungen an Bestellsysteme klassifiziert werden die zur Zeit nur selten implementiert sind, in Zukunft aber immer nicht weg zu denken sein werden wenn E-

Commerce als Vertriebsweg an Gewichtung gewinnt.

6.10.1 Profilbildung

One-to-One-Marketing. Es gibt bereits in einigen Systemen die Möglichkeit, den Benutzer im Zuge seiner Einkäufe oder zumindest seiner persönlichen Angaben in Gruppen einzuteilen. Der Shop-Server stellt das gebotene Warenangebot dann auf den Einkäufer ab. Einfachste Beispiele sind, daß keine Strumpfhosen an Männer und keine PC-Hardware an Apple-Besitzer angeboten werden.

6.10.2 Sonderposten

Bestimmte Güter könnten als Sonderangebote oder Restposten gekennzeichnet und in eine besondere Gruppe aufgenommen werden. Derartige Artikel würden dann etwa auf der Eingangsseite besonders hervorgehoben.

6.10.3 Komplementäre Produkte

Es wäre günstig, wenn bei einzelnen Produkten ein Verweis auf andere, diese ergänzende oder damit zusammenhängende Produkte gegeben werden könnte. Dadurch ließen sich Verbundeffekte nutzen und der Benutzer ließe sich horizontal zur eigentlichen Gliederung der Warengruppen führen. Zusätzlich könnte ein Agent dezent auf diese komplementären Produkte aufmerksam machen, wenn der Benutzer etwas in den Einkaufskorb einfügt.

6.10.4 Komplexe Produkte

Es gibt derzeit keine Möglichkeit, Produktoptionen mit Aufpreisen zu belegen. Das könnte aber z. B. beim Zusammenstellen eines PCs von Vorteil sein. Der Nutzer könnte die Komponenten wie Speicher, Festplatte und Prozessor selber wählen und Preisvergleiche anstellen. Das System berechnet dann jeweils die gewählten Einzelteile.

6.10.5 Empfangsbestätigung

Es ist ein wichtiges und vertrauensschaffendes Merkmal, wenn der Shop-Server nach Erhalt einer Bestellung nicht nur eine Bestätigungsseite ausgibt, sondern auch eine E-Mail an den Kunden absendet. Der Effekt ist, daß kurz nach der Bestellung eine schriftliche, wenn auch nicht rechtsgültige Bestätigung eingeht. Über Gateways wären auch Fax- oder Pager Nachrichten möglich.

6.10.6 Detailliertere Berichte

Es wäre sehr sinnvoll, wenn detaillierte Berichte wie Statistiken nach Warengruppen und Verkaufszeiten, eine Top-Ten Liste der Produkte und Umsatzentwicklungen,

eventuell sogar pro Kunde, erstellt werden könnten. Für zusätzliche Berichte wie eine Berechnung des Rohgewinns müßte man der Datenbank entsprechende Einkaufspreise zufügen können.

6.10.7 Rabattgruppen

Eventuell möchte man die Konditionen für unterschiedliche Kundengruppen variieren. Ein Beispiel wären Nachlässe nach durchschnittlichem Umsatz, die für gute Kunden gewährt werden. Für solche Berechnungen sind aber die Umsätze pro Kunde zu kumulieren und eine Klassifizierung der Kunden in Rabattgruppen vorzunehmen. Das Problem ähnelt damit dem der Profilbildung.

6.10.8 Auftragserstellung

Dieser Punkt hängt eng mit dem Punkt Schnittstellen zusammen. Nach der Annahme von Bestellungen könnte ein spezielles Modul die nachfolgenden Arbeitsgänge veranlassen. Dies könnte in elektronischer Form, in der Art eines Workflow Systems, erfolgen, wäre aber auch als Minimalforderung durch die Erstellung entsprechender Auftragsdokumente zu leisten. Dies würden helfen, die Abwicklung von Aufträgen weiter zu automatisieren.

¹Siehe auch [Abschnitt 4.1 Die Branche, die Produkte](#)

²permanente Direkt-Verbindung

³Siehe auch [Abschnitt 8.3 Sicherheit](#)

⁴Der anbietende Server ist der Rechner, von dem eine HTML-Seite angefordert wird

⁵Laufzeit bedeutet wenn die entsprechende HTML Seite von einem Browser aufgerufen wird

⁶Merchant ist ein von der Firma Lotus Development Corporation entwickeltes Shop-System





Kapitel 7: KOHLHAGE VERBINDUNGSTECHNIK GMBH & CO KG

7.1 Firmenprofil

Die Firma Kohlhage Verbindungstechnik GmbH & Co KG, im folgenden kurz "Kohlhage" genannt, ist Hersteller für Normteile, Einzelteile und Baugruppen aus Metall im Bereich Verbindungstechnik. Kohlhage beschäftigt ca. 70 Mitarbeiter (Stand 08/98), tätigte 1997 Investitionen im Wert von 2 Millionen Mark und erzielte 1997 einen Umsatz von 25 Millionen Mark.

Kohlhage wurde als Metallwarenfabrik zur Herstellung von Schrauben, Muttern und Befestigungselemente im Jahre 1929 gegründet. 1953 und 1970 wurde das Produktspektrum um Drehteile bzw. Umform- und Schweißtechnik erweitert. Heute beliefert sie hauptsächlich die Automobilbranche, die Gummiindustrie und das Baugewerbe.

7.2 Kohlhage und das Internet

Die Internetpräsenz von Kohlhage besteht zur Zeit aus 4 Seiten auf der Website von "Wer-liefert-Was?" (www.kohlhage.wlwonline.de). Hier wird ein Überblick der 4 Produktgruppen gezeigt.

Im Herbst 1997 startete Kohlhage eine Umfrage unter den hundert wichtigsten Kunden. Von den ca. 60 Rückläufern hatten 41 einen Internetzugang im Unternehmen. Von den 20 Kunden die keinen Zugang hatten, haben 11 vor, sich in Kürze einen zu verschaffen. Insgesamt waren 36 bereit, Informationen über Kohlhage im Internet abrufen. 27 Kunden waren auch bereit, Standardartikel über das Internet zu bestellen. Alle 60 sehen im Internet zukünftige Beschaffungs- und Absatzpotentiale für ihre Unternehmen.

Von den 4 Produktgruppen kam nur eine für den Online-Vertrieb in Frage: die Normteile. Um Aufträge der 3 anderen Produktgruppen auszuführen entsteht zwangsläufig ein intensiver Dialog zwischen Kohlhage und dem Kunden. Der Kunde muß Spezifikationen festlegen oder CAD-Zeichnungen erstellen und diese dann Kohlhage zukommen lassen. Kohlhage entwickelt daraus die Konstruktion, legt die Materialien und das Herstellungsverfahren fest. Der Kunde erhält die Konstruktionsdaten im Original und gibt sein Okay. Auf Grund der Komplexität dieser Produkte sind sie nicht geeignet für den Online-Vertrieb.

7.3 Das Bestellsystem

Zusammen mit der Geschäftsführung von Kohlhage wurden die Ist-Analyse und die Anforderungen an das System erarbeitet.

7.3.1 Ist-Analyse

- Die Normteile sind größtenteils nach DIN genormt. Änderungen der Artikeldatenbank sind nur sehr selten notwendig.
- Die Geschäftsführung hatte sich noch nicht auf einen Provider festgelegt bei dem die Seiten abgelegt werden können.
- Die Firma Kohlhage ist nicht vernetzt und verfügt über 2 Online-Zugänge

7.3.2 Anforderungen

- Es sollten keine Verkaufspreise gezeigt werden. Die Site sollte gleichermaßen von Kunden sowie Interessenten genutzt werden können (d.h. ein Nutzer sollte wahlweise eine Bestellung aufgeben oder eine Anfrage starten können). Ein Kunde, der eine Bestellung ohne Verkaufspreise aufgibt, hat in der Regel seine Festpreise für die bestellten Normteile.
- Die Website sollte sich schnell aufbauen.
- Die Website sollte mindestens mit dem Netscape Navigator 3.0 und dem Internet Explorer 3.0 korrekt angezeigt werden können.
- Bestellungen bzw. Anfragen sollen über E-Mail von dem zuständigen Mitarbeiter abgerufen werden.
- Als Nebenprodukt der Diplomarbeit sollte eine neue Homepage für Kohlhage erstellt werden.

7.3.3 Vorarbeit

Da die firmeninterne Artikeldatenbank nicht an das Web angeschlossen werden sollte, lag die Wahl der Datenquelle bei mir. Da noch kein Provider gewählt würde, mußte ich die Datenquelle so wählen, daß sie mit fast jedem System lauffähig ist. Eine SQL-basierte Datenbank ist bei fast jedem Provider vorhanden. Meine erste Überlegung war eine Java-basierte Anwendung, da Java mit JDBC eine Datenbankschnittstelle besitzt. Die JDBC-ODBC Bridge kann mit jeder ODBC-fähigen Datenbank kommunizieren und natürlich auch mit JDBC-fähigen Datenbanken, die immer häufiger zu finden sind. Leider ist JDBC erst ab dem JDK 1.1 implementiert, d.h. ältere Browser, die nur den durch JDK 1.0 definierten Sprachumfang kennen, können damit nichts anfangen. "Ältere Browser" sind die Browser Netscape Navigator und Microsoft Internet Explorer in Versionen älter als 4.0.

Da ich aber meine ersten Versuche hiermit startete und sehr beeindruckt war vom der einfachen Handhabung werde ich die Grundlagen hier kurz vorstellen: JDBC stellt eine Standard-API für Programmierung von Schnittstellen zu Datenbanken mit Java zur Verfügung und ermöglicht somit das Entwickeln von Datenbankanwendungen mit Java. Mit JDBC können Anwendungen für Datenbanken geschrieben werden, die dann z.B. als Client/Server Anwendung auf verschiedenen Plattformen eingesetzt werden können. Das ist besonders interessant für Firmen, die mehrere Filialen haben in denen unterschiedliche Datenbanksysteme auf unterschiedlichen Plattformen laufen. JDBC hat drei Aufgaben:

- Eine Verbindung zu einer Datenbank aufbauen
- SQL-Befehle an die Datenbank senden
- Die Ergebnisse dieser Abfragen verarbeiten

Eine Verbindung zu einer Datenbank aufbauen

Es existieren viele JDBC Treiber. Die JDBC-ODBC-Bridge stellt eine Schnittstelle zu ODBC-Treibern zur Verfügung. Viele Datenbanken, z.B. dBase, Sybase und Oracle, werden mit einem ODBC-Treiber ausgeliefert. Für mSQL, eine UNIX-basierte Datenbank gibt es z.B. den mSQL-JDBC Treiber. Die folgenden Quelltexte werden anhand der JDBC-ODBC-Bridge von Sun Microsystems vorgestellt.

Der benutzte Treiber muß zuerst bei dem JDBC "Driver Manager", das Rückgrat von JDBC, angemeldet werden. Dies geschieht mit folgendem Befehl:

```
Class.forName("sun.jdbc.odbc.JdbcOdbcDriver");
```

Als nächstes wird eine Verbindung "con" vom Typ Connection zur Datenbank aufgebaut. In der Variable "url" steht der Name der Datenbank. Die Datenbank muß vorher bei dem ODBC-Datenquellen-Administrator (unter Windows 95) angemeldet sein:

```
String url = "jdbc:odbc:Verwaltung";
String user = "rebecca";
String pwd = "javatest";
Connection con = DriverManager.getConnection(url, user, pwd);
```

Der Driver Manager übernimmt die angegebene URL und prüft ob der angemeldete Treiber diese URL bearbeiten kann. Ist dies der Fall, so wird die Verbindung erstellt. Die Angaben zum Benutzernamen und zum Paßwort sind optional.

SQL Befehle an die Datenbank schicken

Jetzt wird ein Statement-Objekt stmt des Connection-Objektes erstellt, um SQL-Befehle an die Datenbank zu schicken:

```
stmt = con.createStatement();
stmt.executeUpdate(
"CREATE TABLE Adresse (" +
"name VARCHAR (30), " +
"telefon VARCHAR (15), " +
"plz INTEGER, " +
"ort VARCHAR (20)); "
);
```

Die Ergebnisse der Abfragen verarbeiten

Der obenstehende Quelltext erstellt eine neue Tabelle mit dem Namen: "Adresse". Für diesen SQL-Befehl gibt es keine

Ergebnissätze. Bei einem SELECT-Befehl beispielsweise wird der Befehl "executeQuery" benutzt der eine Datenmenge zurück geliefert. Diese wird in "result" von Typ ResultSet gespeichert.

```
ResultSet result = stmt.executeQuery(
"SELECT name, telefon FROM Adresse ORDER BY name DESC;"
);
```

Mit "result.next();" kann die Ergebnismenge sequentiell durchlaufen werden. Nach dem ersten Aufruf wird auf den ersten Datensatz gezeigt. Der Quelltext mit dem die Ergebnismenge abgerufen werden kann schaut so aus:

```
String name;
String telefon;
while(result.next()) {
name = result.getString("name");
telefon = result.getString("telefon");
System.out.println(name+" hat die Nummer: "+telefon);
} Ein neues Feature von JDBC-Treibern sind Prepared Statements. Diese ähneln den normalen Statements, können aber
Parameter entgegennehmen:
```

```
PreparedStatement pstmt = con.prepareStatement(
"INSERT INTO Adresse (name, telefon) VALUES (?, ?)"
);
```

Die Fragezeichen (?) können zur Laufzeit festgelegt und dann ausgeführt werden:

```
pstmt.setString(1, "Rebecca");
pstmt.setString(2, "0221/660808");
pstmt.executeUpdate();
```

Dann gibt es noch die Callable-Statements. Ein Callable Statement enthält den Aufruf eines Statements und wird in der Datenbank gespeichert.

```
Callable Statement cstmt = con.prepareCall(
"{call getData(?, ?)}"
);
```

Die Fragezeichen stehen für IN-, OUT- sowie INOUT-Parameter. D.h. die Fragezeichen können Parameter an das Statement weitergeben, Ergebnisse entgegennehmen oder sowohl als In- wie auch als Output fungieren.

```
cstmt.registerOutParameter(1, java.sql.Types.VARCHAR);
cstmt.registerOutParameter(2, java.sql.Types.VARCHAR);
cstmt.executeUpdate();
```

Die Verbindung wird nach der Sitzung beendet:

```
Con.close();
[Jepson 1997, S. 48]
```

JDBC hat gegenüber ODBC den Vorteil, daß es eine reine Java Lösung ermöglicht. Außerdem hat ODBC eine C-Schnittstelle und Java müßte mit dieser kommunizieren was einen Verlust an Sicherheit, Stabilität und Plattformunabhängigkeit mit sich bringen würde.

Da JDBC für die Website von Kohlhage leider ausschied, überlegte ich welche Alternativen ich hatte: CGI-Programmierung, Javascript oder ein Shopsystem. Ich ließ mir Proben der Artikeldaten geben und stellte fest, daß folgende Spalten für jedes Produkt vorkommen:

| Hauptgruppe | Artikelnummer | Gewinde | Material |
|-------------|---------------|---------|----------|
| | | | |

Tabelle 9: Auszug aus der Artikeldatenbank von Kohlhage

Je nach Produktgruppe kamen noch weitere spezielle Spalten wie "Durchmesser", "Anzahl Schweißwarzen" usw. vor. Der Inhalt der meisten Spalten ist numerisch. Das war ausschlaggebend dafür, daß ich mich für Javascript entschied. Da die gesamte Datenmenge nur wenige Kilobyte groß ist, überlegte ich, die Daten komplett beim Aufruf der Seiten mit zu laden. Das verlangsamt zwar den ersten Aufruf, aber das Bestellsystem ist wesentlich schneller als eines mit CGI. Und zweitens sind die Seiten auf jedem Server ablegbar und die Firma Kohlhage somit unabhängig von einem Provider bzw. seine spezifischen Systemen.

7.3.4 Implementierung

Das Grobkonzept wurde auch mit der Geschäftsführung von Kohlhage erarbeitet. Die Website sollte in drei Hauptkategorien verlinken wie in Abbildung 6:

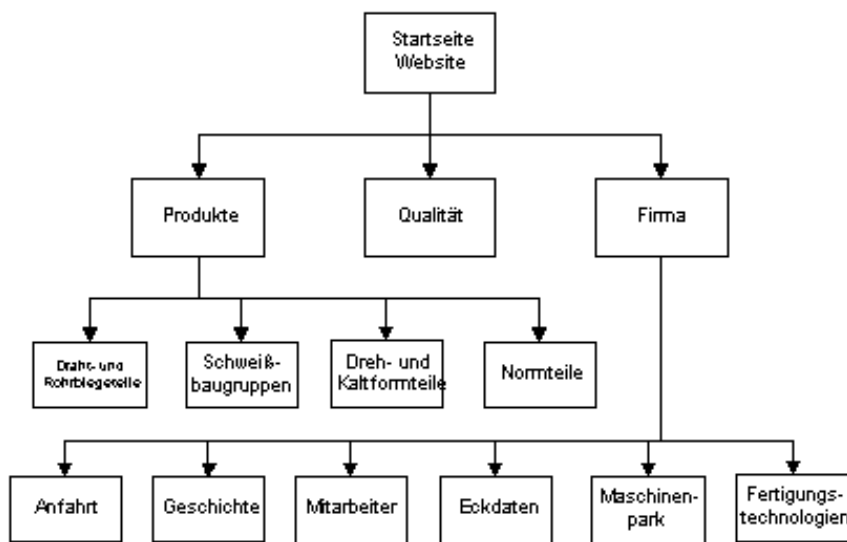


Abbildung 6: Hierarchische Struktur der Website

"Firma" sollte zu Seiten linken, die u.a. Mitarbeiter vorstellen, die Anfahrt beschreiben und weitere Informationen zur Firma bereitstellen. Unter "Qualität" sollten die wichtigsten Zertifizierungen, Auszeichnungen und Referenzen genannt werden. Die Kategorie "Produkte" führt zu vier Unterkategorien mit den vier Produktgruppen. Für die ersten drei Produktgruppen sind statische Info-Seiten vorgesehen. Die Kategorie "Normteile" führt dann zu dem Bestellsystem. Es sollte ein Menu angezeigt werden mit den gängigsten Normteilen. Der typische Ablauf einer Kundenbestellung für Kohlhage wird in Abbildung 7 gezeigt.

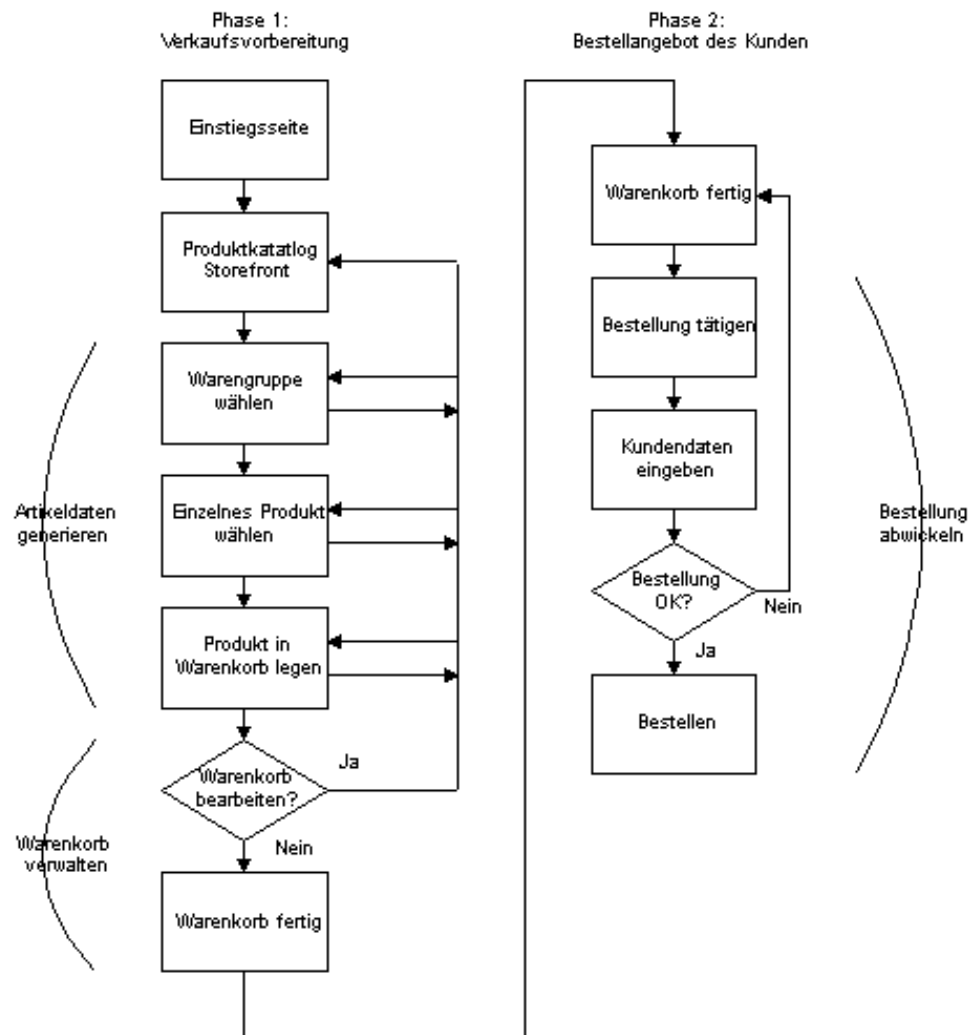


Abbildung 7: Ablauf einer Kundenbestellung

Die 1. Phase einer Online-Bestellung, die der Verkaufsvorbereitung, ist komplett umgesetzt worden. In der 2. Phase, das Bestellangebot des Kunden, entfällt die Berechnung der Endsumme da die Verkaufspreise nicht Teil des Bestellsystems sind. Die 3. Phase der Zahlung und Lieferung entfällt komplett, da weder online bezahlt noch online ausgeliefert wird. Die 4. Phase der Aftersales wird für Kohlhage Website nicht online umgesetzt. Eventuell anfallende Supportanfragen werden telefonisch bearbeitet.

Auf der Basis von Abbildung 7 kann die Erstellung des Bestellsystems in drei Bereiche aufgeteilt werden, nämlich:

- Die Verwaltung der Artikeldaten
- Die Verwaltung des Warenkorbs
- Die Bestellung

Auszüge des Quellcodes können im Anhang A eingesehen werden.

7.3.4.1 Die Verwaltung der Artikeldaten

Die Verzweigung Produkte --> Normteile führt zu dem Bildschirm in Abbildung 8.

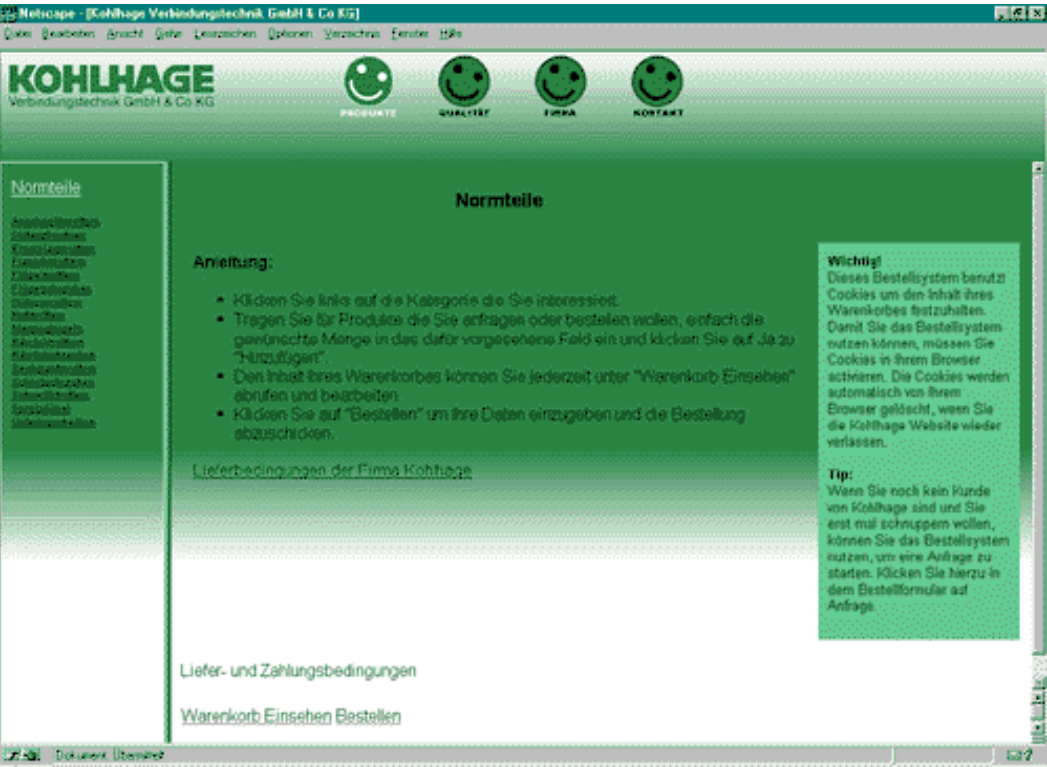


Abbildung 8: Startmaske des Bestellsystems

Der Bildschirm besteht aus der horizontalen Hauptnavigationsleiste oben, eine Subnavigationsleiste links, eine Kontrolleiste unten und dem Anzeigebereich in der Mitte. Eine Datei namens "data.htm" wird versteckt mit geladen wenn diese Seite aufgerufen wird. Sie enthält alle Artikeldaten.

Die Datei "data.htm" enthält eine "comma-seperated-values" Datensammlung der Artikel. Jeder Artikel besteht aus einem versteckten Feld mit einer laufenden Nummer (NAME) und einem Wert (VALUE) der sich wie in Tabelle 10 dargestellt zusammensetzt. Die einzelnen Werte werden in einer vordefinierten Reihenfolge mit Semikola getrennt aufgezählt.

| | |
|----------------------------------|--|
| Artikelgruppe;Untertitel;Grafik; | Diese Werte bilden den Kopf der Seite. Die Artikelgruppe und der Untertitel werden als Titel dargestellt und die Grafik darunter angezeigt. |
| Anz. Reihen; Anz. Spalten; | Die Anzahl der Reihen und Spalten sind wichtig weil die Tabelle dann schneller aufgebaut werden. |
| Artikelnummer;Gewinde;Material; | Diese drei Spalten kommen für jeden Artikel vor. Danach werden die individuellen Spaltenbezeichnungen aufgezählt. Die Anzahl muß mit der Anzahl der Spalten übereinstimmen. Jetzt folgt für jeden Artikel eine eigene Zeile mit den dazugehörigen Daten. Die Reihenfolge der Daten muß der der Spaltenbezeichnungen entsprechen. |

Tabelle 10: Inhalt eines VALUE Tags in data.htm

Der folgende Code ist ein Beispiel für den Artikel "Anschweißmuttern" mit dem Subtitel "(Anpunktmuttern) mit durchgehendem Gewinde - Tiefziehbandstahl". Die dazugehörnde Grafik heißt "flanschm.gif". Es werden 6 Zeilen und 7 Spalten eingelesen. Zusätzlich zu den 3 allgemeinen Spalten hat der Artikel noch die Eigenschaften "(e)", "(h)", "(s)" und "Anzahl der Schweißwarzen".

```
<INPUT TYPE="hidden" NAME="1" VALUE="
Anschweißmutter;(Anpunktmuttern) mit durchgehendem Gewinde -
Tiefziehbandstahl;flanschm;
6;7;Artikelnummer;Gewinde;Material;(e);(h);(s);Anzahl der Schweißwarzen
;010001;M3;stahl;17;6;9;2
;010002;M4;stahl;17;6;9;2
;010003;M5;stahl;19;8;11;2
;010004;M6;stahl;19;8;11;2
;010005;M8;stahl;26;11;18;4
;010006;M10;stahl;26;12;18;4
;">
```

Die darauffolgenden Zeilen sind der Inhalt der Artikel-Tabelle. Nach Aufruf eines Artikels erscheint ein Bildschirm wie ihn Abbildung 9 zeigt. Der hier ausgewählte Artikel ist die Flanschmutter. Zu diesem Artikel gibt es keinen Subtitel. In einer "comma-separated-values" Datensammlung werden fehlende Daten einfach mit einem Leerzeichen und das Semikolon dargestellt.

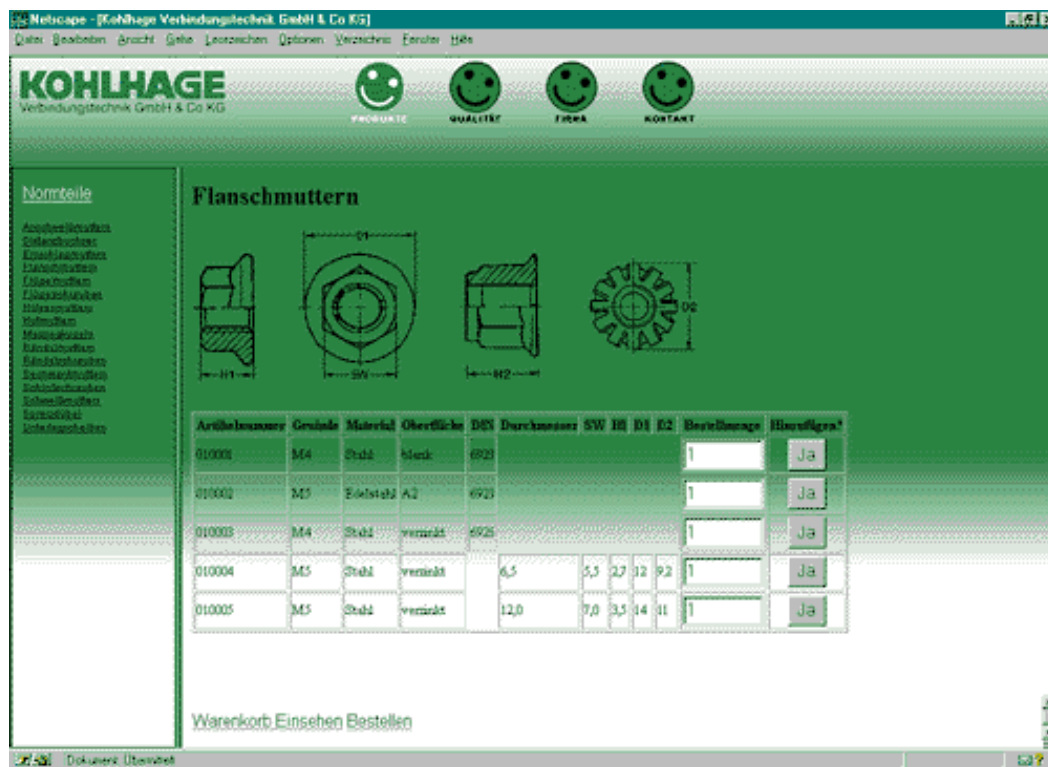


Abbildung 9: Aufbereitete Artikeldaten

7.3.4.2 Verwaltung des Warenkorbs

Der letzte Bildschirm, Abbildung 9, zeigte die zur Bestellung verfügbaren Varianten des Artikels "Flanschmutter". In das Feld "Bestellmenge" muß der Kunde die gewünschte Menge eintragen und mit dem Button "Hinzufügen: Ja" bestätigen.

Der Warenkorb muß die ausgewählten Artikel zusammen mit der gewünschten Menge verwalten. Der Kunde soll jederzeit den aktuellen Stand abrufen können und die einzelnen Artikel löschen oder die eingetragenen Mengen ändern. Es gibt zwei Möglichkeiten, den Inhalt des Warenkorbes festzuhalten, nämlich auf dem anbietendem Server oder auf seiten des Clients. Die Alternative mit dem Server hat den Nachteil, daß der Datenverkehr zwischen dem Server und dem Client verstärkt wird. Bei jeder Änderung des Inhaltes müssen die Daten wieder an den Server geschickt werden. Und umgekehrt bei jedem Abruf des Inhaltes. Die Verwaltung des Warenkorbes auf Seitens des Clients basiert auf der Cookie-Technik. Diese Alternative hat den Nachteil, daß Cookies einen sehr schlechten Ruf¹ haben und die Nutzer ggfs. das Setzen von Cookies aktivieren müssen bevor das Bestellsystem funktionieren kann. Der Vorteil liegt in den kürzeren Antwortzeiten.

Für das Kohlhage Bestellsystem wurde die Cookie-Technik benutzt, da diese Methode unabhängig ist vom dem eingesetzten Server. Für jeden Cookie können die folgenden Felder belegt werden:

| | |
|----------------|---|
| NAME=VALUE; | Name und Wert des Cookies werden hiermit festgelegt |
| domain=DOMAIN; | Die Domäne die das Cookie setzt. Defaultmäßig wird der Domännamen des anbietenden Servers gesetzt. |
| path=PATH; | In "path" können Pfade von URLs angegeben werden, die den Cookie auslesen darf. Defaultmäßig wird der Pfad des anbietenden Servers gesetzt. |
| secure | Die Angabe von "secure" legt fest, ob der Cookie gesichert übertragen werden soll. |
| expires=DATE; | Das Ablaufdatum des Cookies kann hiermit festgelegt werden. Folgendes Format ist vorgeschrieben: Wdy, DD-Mon-YYYY HH:MM:SS GMT. |

Tabelle 11: Die Felder eines Cookies

Der Netscape Browser erlaubt das Setzen von 20 Cookies à 4 Kbyte pro Domäne. Der Microsoft Internet Explorer aber erlaubt nur ein Cookie pro Domäne. Da das Bestellsystem mindestens auf diesen beiden Browsern laufen sollte, mußte diese Einschränkung überwunden werden. Der Cookie wird also wie folgt aufgebaut:

Warenkorb=[artnr|artname|gewinde|material|menge];

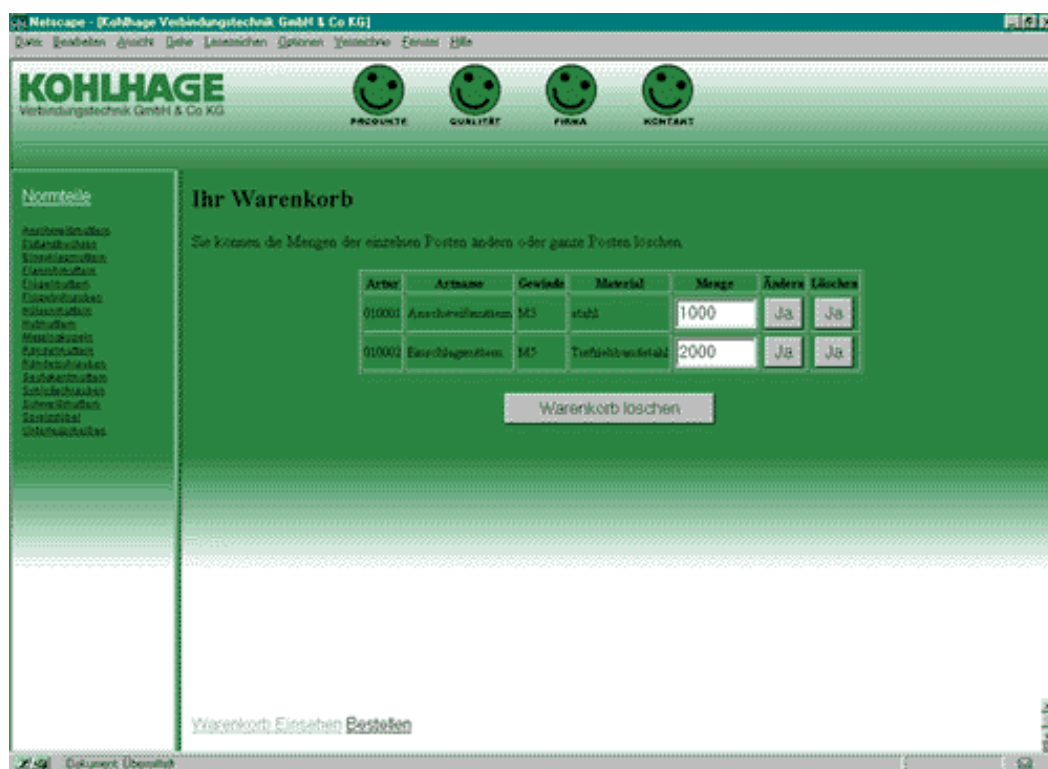
Er bekommt den Namen "Warenkorb" und für jeden ausgewählten Artikel werden die Eigenschaften Artikelnummer, Artikelname, Gewinde, Material und Menge als Wert gespeichert. Kommt ein zweiter Artikel dazu, so wird das Ende des Cookies ermittelt und die neuen Daten angehängt wie folgt:

Warenkorb=[artnr|artname|gewinde|material|menge][artnr|artname|gewinde|material|menge];

Die eckigen Klammern "[" kennzeichnen den Anfang und das Ende der Artikel und die Striche "|" unterteilen die einzelnen Eigenschaften.

Wenn der Kunde seinen Warenkorb abrufen, wird der Cookie Artikel für Artikel ausgelesen und in Zeilen dargestellt. Abbildung 10 zeigt den Warenkorb mit zwei enthaltenen Artikeln. Der Kunde hat drei Möglichkeiten den Warenkorb zu editieren:

1. Die Mengen der Artikel einzeln zu ändern
2. Ein Artikel ganz aus dem Warenkorb zu löschen
3. Den gesamten Warenkorb zu löschen





Kapitel 8: WIE SIEHT DIE ZUKUNFT AUS?

8.1 Mögliche Richtungen des Internets

Die Zukunft des Internets ist nicht einfach vorauszusehen. Dataquest erwartet, daß die Zahl der Internetfähigen Rechner in Europa im Jahr 2000 auf 69 Millionen steigen wird (13,3 Millionen in 1997) [CZ 34 1998, S. 2]. Im Folgenden werden ein paar Richtungen aufgezeigt.

8.1.1 Lebensmittelhändler im Internet

Auf der Website der Firma [Peapod](#) in Amerika kann ein Kunde einen Einkaufszettel mit seinen Einkaufswünschen erstellen und bei Peapod in Auftrag geben. Peapod kauft dann die Lebensmittel ein. Sonderangebote werden an den Kunden weitergegeben, Coupons können auch eingelöst werden. Geliefert wird die Ware zu einer vom Kunden festgelegten Uhrzeit und an jedem Tag der Woche. Nutzer erzählen, daß sie z.B. dann bestellen wenn sie auf Geschäftsreise sind, damit sie nach ihrer Heimkehr frische Lebensmittel haben [Peapod 1998].

Die Karstadt AG bietet unter www.myworld.de einen ähnlichen Service in Deutschland an. Dieser ist im Großraum Essen (Bottrop, Gelsenkirchen, Gladbeck, Mülheim und Oberhausen) verfügbar. Die Filialen München, Frankfurt/Main, Hamburg und Berlin sind noch in Bearbeitung. Bei Bestellungen bis 100 Mark sind zehn Mark Versandkosten veranschlagt. Darüber hinaus werden keine Versandkosten berechnet. Bücher werden kostenlos verschickt. Ausgeliefert wird Montags bis Freitags zwischen 9 und 21 Uhr und Samstags zwischen 9 und 18 Uhr. Dabei kann der Käufer den Lieferzeitraum auf ein paar Stunden festlegen, beispielsweise zwischen 9 und 12 Uhr.

"Ihnen fehlt die Zeit zum Einkaufen? Kein Problem, wir haben die Lösung für Sie. Von nun an können Sie von der Butter bis zum Champagner, Lebensmittel online bestellen." [Karstadt 1998]

Trotzdem lohnt es sich noch die Lebensmittel in dem Supermarkt nebenan zu beziehen da die Preise der Karstadt AG relativ hoch sind. Weitere Online-Geschäfte sind Kaiser's unter www.kaisers.de/bestell/ und www.onkelemma.de.

Auf der Website www.germany-service.com können deutsche Produkte bestellt und an fast jede Ecke der Welt verschickt werden. Sie versprechen: *"Your fast help for all you need from Germany"*. Zehn Flaschen Paulaner Weißbier kosten beispielsweise 39 Dollar zuzüglich Versandkosten.

8.1.2 Informationssystem

Das Internet hat das Potential eine informierte Öffentlichkeit herzustellen. Es ist relativ billig und es ist relativ leicht zu nutzen. Die Bedeutung des freien Zuganges zu Informationen wird eine immer größere Rolle im öffentlichen Bewußtsein spielen. Unter quake.wr.usgs.gov/recenteqs/ können beispielsweise Informationen über Erdbeben abgerufen werden. Das amerikanische seismologische Institut "US

Geological Survey" (USGS) betreibt diese Website. Die Daten werden ständig aktualisiert. Interessierte können sich hier über Erdbeben informieren und analysieren, ob ihr Wohngebiet besonders gefährdet ist. Außerdem werden ab einer bestimmten Erdbebenstärke Warnmeldungen ausgegeben.

8.1.3 E-Bücher

Bücher aus dem Internet laden. Das Rocketbook ist ein Produkt der Bertelsmann AG. Es ist ein buchgroßes elektronisches Lesegerät das per serieller Schnittstelle an den PC angeschlossen werden kann. Es soll bis zu 4000 Seiten im Hauptspeicher halten können. Und das Lesematerial? Das wird natürlich aus dem Internet gezogen. Eine spezielle Verschlüsselungstechnik verhindert dabei, daß ein gekauftes Buch unberechtigt kopiert oder weitergegeben wird. Geplant ist, das E-Buch noch in diesem Jahr auf dem Markt zu bringen [c't 15/98, S. 39].

8.1.4 Dolmetscher-Browser

Inzwischen gibt es Software die, in den Browser integriert, die Texte auf den HTML-Seiten vom Französischen ins Deutsche übersetzen. Die Software der Kölner Firma Heisoft beispielsweise ist als Übersetzungsbrowser konzipiert, der das Gefühl erzeugt, in einem deutschen Internet zu surfen [CZ 32 1998, S.13].

8.1.5 Virtuelle Unternehmen

Virtuelle Unternehmen mit minimaler physischer Infrastruktur sind denkbar. Softwareprojekte deren Entwicklungsteams über das Internet zusammengestellt und koordiniert werden sind heute schon Alltag.

Manche Rathausgänge könnten auch über das Internet abwickelt werden. Noch dienen die Online-Sites der Kommunen meist nur der eigenen Präsentation (Stadtgeschichte) oder als reine Informationssysteme (Straßenkarten, Veranstaltungskalender, Fahrpläne u.v.m.) Denkbar ist das "One-Stop-Government" das als Synonym für eine bürgernahe, zeitlich und räumlich flexible Behörde mit einem möglichst breiten Aufgabenspektrum steht. Der Bürger sollte im Internet seinen Personalausweis verlängern lassen können oder Wohngeld beantragen können usw. [c't 9/98, S. 64 f.].

Ein Studium an einer Online-Universitäten, das über das Internet abgewickelt wird ist schon Realität. So ein Studium bietet Chancen für die interessierte Hausfrau wie auch als Weiterbildungsmaßnahme für Berufstätige. Beispiele hierfür sind die FernUni Hagen (www.fernuni-hagen.de) und die TU Chemnitz-Zwickau (rnvs.informatik.tu-chemnitz.de/dfn) mit ihrem Projekt Internet-Fernstudium.

8.1.6 Intelligente Softwareagenten

Einen Softwareagenten¹, der Kunden durch den virtuellen Shop begleiten und beim Einkauf berät, findet sich unter www.medienparadies.de wo CD's und Bücher angeboten werden. Dort fragt die freundliche Schlange Lydia nach den Wünschen und gibt Kaufempfehlungen. Außerdem kann man sich mit Lydia auf Smalltalk einlassen - ihr Hobby ist die Astrologie. Noch verlaufen die Gespräche nach einem ganz einfachen Muster und werfen kein gutes Licht auf das KI-Programm, das hinter Lydia stehen soll [c't 11/98 (2), S. 142].

Preisagenten, die für den Surfer Angebote im Internet vergleichen und den günstigsten Anbieter eines

Produktes ermitteln, gibt es von verschiedenen Firmen. Der erste Preisvergleichser war der an der Universität Washington von Wirtschaftswissenschaftlern entwickelte [Shop-Bot](#), der eigentlich nur das Spiel von Angebot und Nachfrage illustrieren sollte. Inzwischen gibt es beispielsweise von Continuum Software den [Fido](#). Forscher des Watson Research Center der IBM untersuchten die Funktionsweise solcher Agenten (http://www.research.ibm.com/infoecon/paps/html/alife6/alife6_public.html). Sie fanden heraus, daß die Suche eine gravierende Schwachstelle hat, die sie als Zero memory bezeichnen. Die Software-Agenten achten allein auf günstige Preise. Die Bonität, Lieferfähigkeiten oder -schwierigkeiten der beteiligten Firmen werden dabei völlig ausgeklammert. Nach Ansicht der Forscher werden die Anbieter zwangsläufig ein Kartell bilden, das die Preise kontrolliert. [CZ 31 1998, S. 12].

8.2 Zahlung

Unverzügliche Auslieferung oder auch 24 Stunden Lieferung sind gegen Vorkasse gar nicht möglich bei einer Online-Bestellung und die Lieferung per Nachnahme ist mit Gebühren verbunden. Online-Zahlungsverfahren haben hier klare Vorteile. Das Internet erfordert ein mediengerechtes Zahlungsmittel, damit der Händler sein Geld unverzüglich erhält und er dem Kunden die Ware (wenn es sich um Information oder Software handelt) bedenkenlos übergeben kann.

Der folgende Teil der Erhebung von [Kurbel 1998] sollte Aufschluß über den heutigen Stand der Zahlungsmittel bei WWW-Geschäften geben. Die Unternehmen wurden gefragt, wie sie den Vorgang der Bezahlung von Leistungen gestalten, die sie über das Internet bestellen oder vertreiben. Tabelle 12 zeigt, daß elektronische Zahlungsmittel kaum gebräuchlich sind (2,7 %). Offensichtlich gibt es Vorbehalte oder die technischen Voraussetzungen für sichere Zahlungswege liegen noch nicht vor. 52,6 % bevorzugen die konventionelle Zahlung auf Rechnung [Kurbel 1998].

| % | Zahlungsweise |
|------|---------------------|
| 52,6 | Rechnung |
| 25,4 | Bankeinzug |
| 17,6 | Scheck |
| 16,6 | Kreditkarte |
| 2,7 | Elektronisches Geld |
| 12,0 | Andere |

Tabelle 12: Bezahlung von Leistungen über das WWW

Drei Anforderungen müssen beim Online-Bezahlen erfüllt sein:

- Die Vertraulichkeit und
- Integrität von Bestell- und Zahlungsinformationen sowie
- die Authentifizierung von Händler und Kunde.

Die Verfahren zur Online-Zahlung können in zwei Kategorien aufgeteilt werden: "Stored-Account"-

Verfahren (Konto lagernd) und "Stored-Value"-Verfahren (Wert lagernd).

8.2.1 Stored-Account Verfahren

Bei den Stored-Account Verfahren verläßt der Geldwert einer Transaktion nie die Tresore der Banken. Der Kunde bestellt ein Produkt und weist den Händler an, den Betrag von seinem Konto abzubuchen. Der Geldwert wird also lediglich von dem Konto des Kunden auf das Konto des Händlers transferiert. Daher ist die Sicherheit solcher Verfahren auch höher, denn das Geld verläßt nie die Bank und die Zahlungstransaktionen sind nachvollziehbar. Die Gegenseite ist der Verlust der Privatsphäre für den Kunden.

8.2.1.1 Die Kreditkarte

In den USA ist die Kreditkarte derzeit die gebräuchlichste konventionelle sowie auch Online-Zahlungsform. Sie hat den Vorteil, daß international getätigte Geschäfte problemlos abgewickelt werden können. Doch auch diese Form erfüllt nicht alle drei Anforderungen. Der Händler hat das Risiko, daß die Informationen gefälscht oder die Karte gestohlen und womöglich gesperrt ist. Der Kunde, auf der anderen Seite, muß dem Händler dahingehend vertrauen, das dieser nur den Betrag abbucht, der auch auf der Website ausgewiesen war. Zudem speichert der Händler die Kundendaten auf seinem System ab. Der Kunde kann nur hoffen, daß der Händler sein System genügend gegen Hacker abgesichert hat.

1996 wurde ein Standard namens SET (Secure Electronic Transaction) definiert, der die Bezahlung mit der Kreditkarte im Internet sicherer macht als im richtigen Leben. Dabei besitzen Händler und Kunde fälschungssichere Zertifikate, die die Identität beider sicherstellt. Bei einem Zahlungsvorgang verschlüsselt die Software auf Kundenseite den Rechnungsbetrag und die Kreditkartendaten, packt das Kundenzertifikat dazu und schickt dieses Paket mit einer Signatur versehen an den Händler. Der kann es nicht einsehen, sondern fügt lediglich sein Zertifikat sowie eine weitere Signatur hinzu und verschickt das ganze an einen sogenannten Prozessor. Der entschlüsselt das Paket, gleicht die Daten mit der Kreditkartengesellschaft ab und sendet im Erfolgsfall dem Händler und dem Kunden eine signierte Bestätigung des Geldtransfers. Dabei sichern die Zertifikate die Authentizität und die Signaturen die Integrität. Da der Händler keine Kreditkartendaten erhält und der Prozessor nichts über die gekaufte Ware erfährt, ist auch die Vertraulichkeit gesichert.

Mittlerweile bieten immer mehr Hersteller SET-Software an, so z.B. IBM, Verifone und Brokat. Der Standard genießt ein hohes Vertrauen, da die verwendeten Verfahren offengelegt wurden.

Die amerikanischen Firmen [First Virtual \(FV\)](#) und [Cybercash](#) haben ihre eigenen Stored-Account Zahlungsverfahren entwickelt. FV benutzt ein ganz einfaches Verfahren. Beteiligte Firmen und Kunden müssen vor der Transaktion bei FV angemeldet sein. Wenn ein solcher Kunde bei einem beteiligten Händler ein Produkt kaufen möchte, fragt der Händler die VirtualPIN des Kunden ab. Wenn diese gültig ist, wird das Produkt ausgeliefert. Der Händler schickt dann die Daten des Kaufs an FV. FV schickt dem Kunden eine Aufforderung zur Bestätigung des Kaufs. Geht die Bestätigung ein, wird die Kreditkarte des Kunden belastet. Der Händler erhält sein Geld jedoch erst nach 90 Tagen. Diese 90 Tage gelten auch als Rückgabefrist für den Kunden. Die Vorteile dieses Systems liegen darin, daß die Kreditkartendaten nicht übers das Internet verschickt werden müssen. Außerdem werden die Daten des Kunden nicht auf jedem Händler-Webserver gespeichert sondern nur bei der FV.

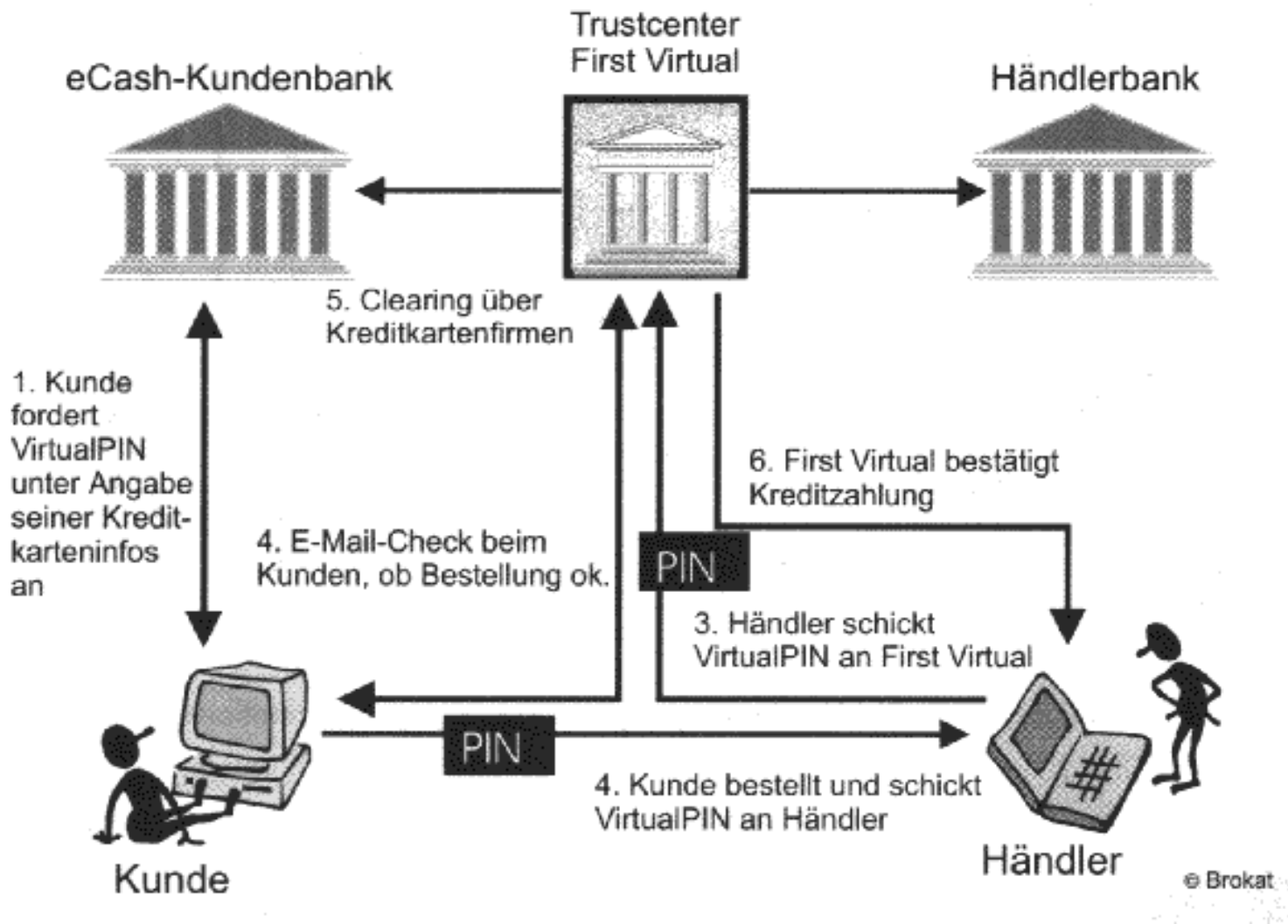


Abbildung 12: Das Online-Zahlungsverfahren von First Virtual

Das attraktivste Feature an diesem Verfahren ist die Einfachheit. Es müssen keine Programme installiert werden und die vorhandenen Kreditkarten Infrastrukturen werden genutzt. Cybercash hat ein ähnliches System entwickelt, CyberCoin. Auch hier müssen beide Geschäftspartner bei Cybercash registriert sein. Der Kunde übermittelt dem Händler seinen Kaufwunsch und schickt mit Hilfe des Cybercash Programms die Zahlungsdaten. Diese sind mit dem Public-Key² von Cybercash verschlüsselt. Der Händler leitet diese weiter an Cybercash. Hier werden sie entschlüsselt und eine Anfrage wird an die Bank oder das Kreditkarteninstitut des Kunden geschickt. Die Zahlungsgenehmigung oder -ablehnung wird von dem Geldinstitut zurück an Cybercash übermittelt und weiter zu dem Händler. Der Händler hat bei diesem Verfahren den Vorteil, daß er sofort darüber Bescheid bekommt, ob die Bezahlung in Ordnung geht. Der Datenverkehr zwischen Cybercash und den Geldinstituten läuft nicht übers Internet sondern über private Netzwerke und ist somit sicher vor Angriffen aus dem Internet. Auch bei diesem Verfahren bekommt der Händler die Zahlungsdaten des Kunden nicht zu sehen. Diese werden ausschließlich bei Cybercash gespeichert. CyberCoin eignet sich für Micropayments. Anwendungsmöglichkeiten für solche Kleinbeträge sind beispielsweise der Verkauf von Grafiken online oder Pay-per-View Websites, beispielsweise Anzeigenmärkte³ die eine Gebühr erheben für das Anzeigen ihrer Webseiten.

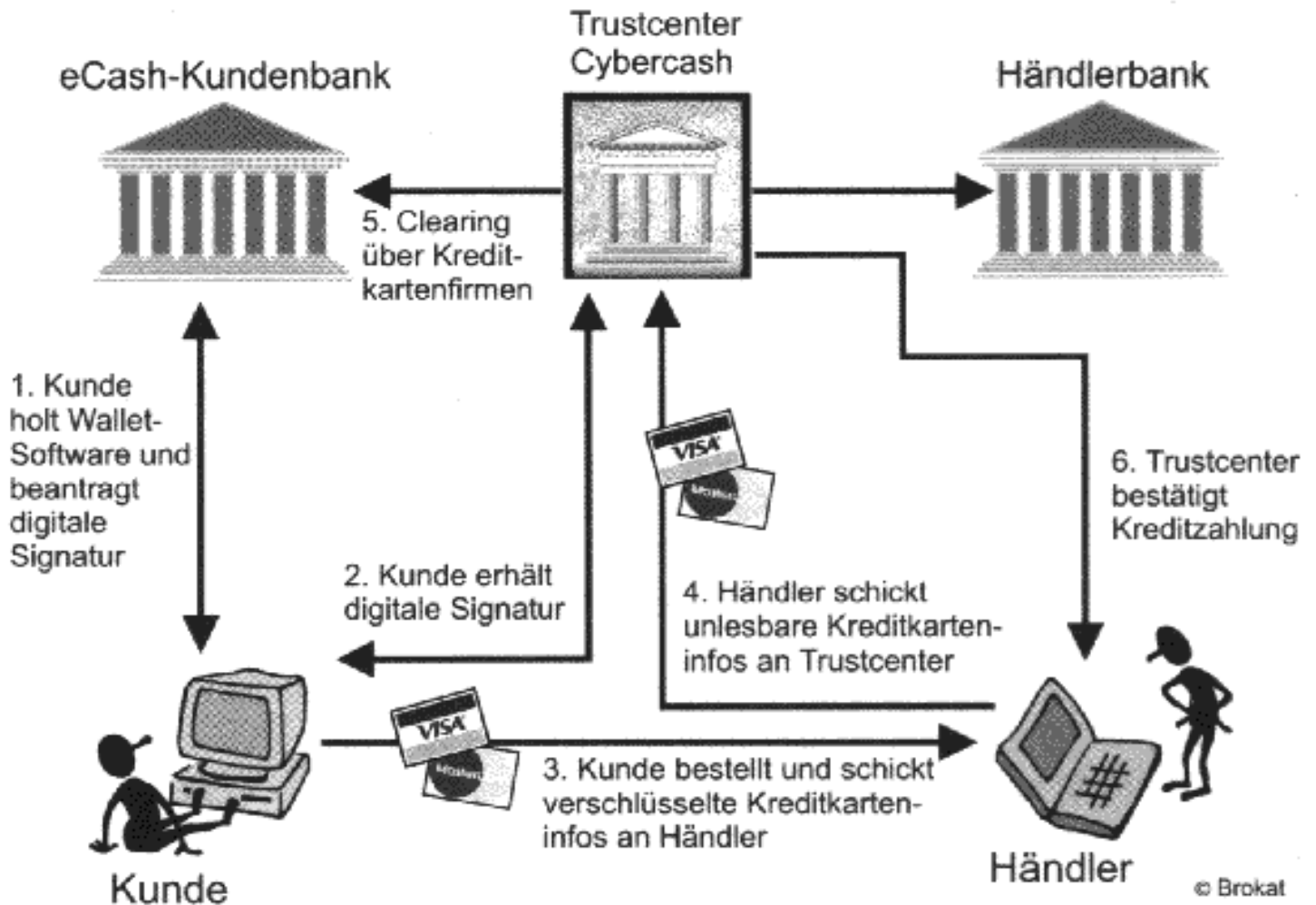


Abbildung 13: Das Online-Zahlungsverfahren von CyberCash

Ein Nachteil ist, daß zusätzliche Software zu installieren ist. Außerdem haben beide Verfahren den Nachteil, daß die Einkaufsgewohnheiten der beteiligten Kunden protokolliert werden könnte. Es können Profile erstellt werden anhand der Daten die dann als Basis für gezielte Werbemaßnahmen genutzt werden könnten. Solche Vertrauensbrüche sind zur Zeit aber nicht bekannt und FV gibt an über 180.000 Käufer und 2.650 Händler zu betreuen. Ab Anfang 1999 will die Hypo-Vereinsbank mit CyberCash "Ernst machen" und als erste deutsche Bank die Pilotphase beenden.

8.2.1.2 Elektronische Lastschrift

Das elektronische Lastschriftverfahren (electronic direct debit) basiert in Deutschland auf einer virtuellen Buchungskarte für die der Kunde einmalig einen schriftlichen Einziehungsauftrag erteilt. Dann erteilt der Kunde von Fall zu Fall seine Einwilligung zur Abbuchung von seinem Konto zugunsten des betreffenden Händlerkontos. Es ist allerdings noch umstritten, ob diese Variante der Bezahlung für den Kunden rechtlich bindend ist. Grundvoraussetzung ist in jedem Fall, daß die Einwilligung des Kunden für jeden Vorgang nachweisbar dokumentiert ist. Die Verwendung der Digitalen Signatur⁴ erscheint daher unerlässlich.

8.2.2 Stored-Value Verfahren

Diese Verfahren ersetzen die Währung mit dem digitalen Gegenstück. Im Gegensatz zu den Stored-Account Verfahren, bei denen das Geld in der Bank bleibt, wird bei den Stored-Value Verfahren das

Konto in der Bank belastet um den entsprechenden Wert auf PC oder Smartcards⁵ zu übertragen. Der Geldwert verläßt also die Bank. Ziel ist es die Privatsphäre des Kunden zu wahren und die Online-Zahlung der realen Cash-Zahlung anzunähern. Diese Verfahren sind sogar anonym als eine Barbezahlung, weil die Beteiligten sich nicht gegenüberstehen müssen.

8.2.2.1 Die EC-Geldkarte

Bankdienstleister wie TeleCash, Brokat Systeme GmbH und Ikoss Van GmbH hoffen auf den Einsatz der EC-Geldkarte als Online-Zahlungsmittel. Die mit einem Chip versehene Karte kann mit bis zu 400 Mark aufgeladen werden. Der entscheidende Vorteil gegenüber der Kreditkarte ist die Möglichkeit, auch Micropayments wirtschaftlich abzurechnen. Außerdem ist die Anonymität des Käufers gegenüber dem Händler beim Bezahlen mit der EC-Geldkarte gewahrt. Möglich wäre auch die Speicherung der Private-Keys⁶, die für Verschlüsselungen notwendig sind, auf der Karte und somit nicht auf dem Rechner, wo vielleicht auch andere Zugang haben. Der Einsatz setzt allerdings einen Chipkartenleser voraus. Die schnell fortschreitende Verbreitung von Chipkarten aller Art dürfte dafür sorgen, daß Kartenleser bald zur Standardausrüstung von PC's gehören, etwa als integraler Bestandteil der Tastatur (wie beispielsweise in vielen Arztpraxen). Der ZKA (Zentraler Kredit Ausschuß) verweigert allerdings noch seine Zustimmung bezüglich der Nutzung der Geldkarten wegen vorhandener Standardisierungslücken. Richtig bequem wird diese Methode wenn das Aufladen des Chips auch am heimischen PC über das Internet möglich ist. Die Unternehmen Bull AG, Ikoss Van GmbH und ESD Information Technology Entwicklungs GmbH haben den Prototyp eines virtuellen Ladenterminals entwickelt, welches das Aufladen der Geldkarte im Rahmen des HBCI-Standards übers Internet ermöglicht.

Zwei schon eingesetzte Smartcard Zahlungsverfahren sind die Mondex Karten von [Mondex](#) mit der Unterstützung von MasterCard International und Visa Cash von der Visa Kreditkarte.

8.2.2.2 Digitales Geld

Echtes Bargeld wechselt täglich den Besitzer ohne das bei jeder Transaktion eine Autorisierung und die Echtheit des Zahlungsmittels ausgewiesen werden muß. Elektronisches Geld muß Echtheit und Autorisierung der ausgebenden Stelle nachweisen um als Zahlungsmittel gelten zu können.

Die Deutsche Bank testete als erstes Geldinstitut in Deutschland den Einsatz und die Akzeptanz von elektronischem Geld in einem Pilotversuch. Rund 1.500 Kunden und ca. 35 Händlern sollten von Oktober 1997 bis Januar 1998 direkt auf dem elektronischen [Internet-Marktplatz](#) Waren und Dienstleistungen per Mausklick einkaufen und verkaufen können.

Das verwendete eCash -Verfahren der niederländischen Firma [DigiCash B.V.](#) wurde seit Herbst letzten Jahres im internen Pilotbetrieb erfolgreich getestet. Bereits 1995 war das Verfahren von der Europäischen Kommission mit dem "Information Technology European Award" ausgezeichnet worden. eCash eignet sich vor allem für die Zahlung kleinerer Beträge.

Der Kunde hat es grundsätzlich mit drei Konten zu tun: sein konventionelles Girokonto, ein neues eCash Konto und die eCash Geldbörse auf seinem PC. Bis zu 400 Mark kann von dem eCash-Konto in die Geldbörse überwiesen werden. Dazu werden elektronische Münzen auf dem heimischen PC erstellt. Diese werden von der Bank unterschreiben (ohne das diese die Seriennummern kennt). Jetzt kann der Kunde jederzeit bei den teilnehmenden Internet-Shops online einkaufen. Der Vorgang ist denkbar einfach: die

Ware wird per Mausklick ausgewählt, der Kauf erfordert nur eine weitere Bestätigung über den geordneten Gegenstand, den Händler und den Betrag. Der Händler schickt die Münzen weiter an seine Bank die die Unterschrift prüft und die Seriennummern registriert. Dem Händler werden dann die elektronisch erhaltenen Beträge sofort gutgeschrieben. Weder er noch die Bank können jedoch nachvollziehen, welcher Kunde den Kauf getätigt hat. Zur Sicherheit für Käufer und Händler verwendet das Verfahren komplexe kryptographische Verschlüsselungen. Die elektronischen Münzen werden mit einer sogenannten elektronischen Unterschrift versehen, die die Echtheit der Münzen garantiert und die in der Praxis nicht gefälscht werden kann.

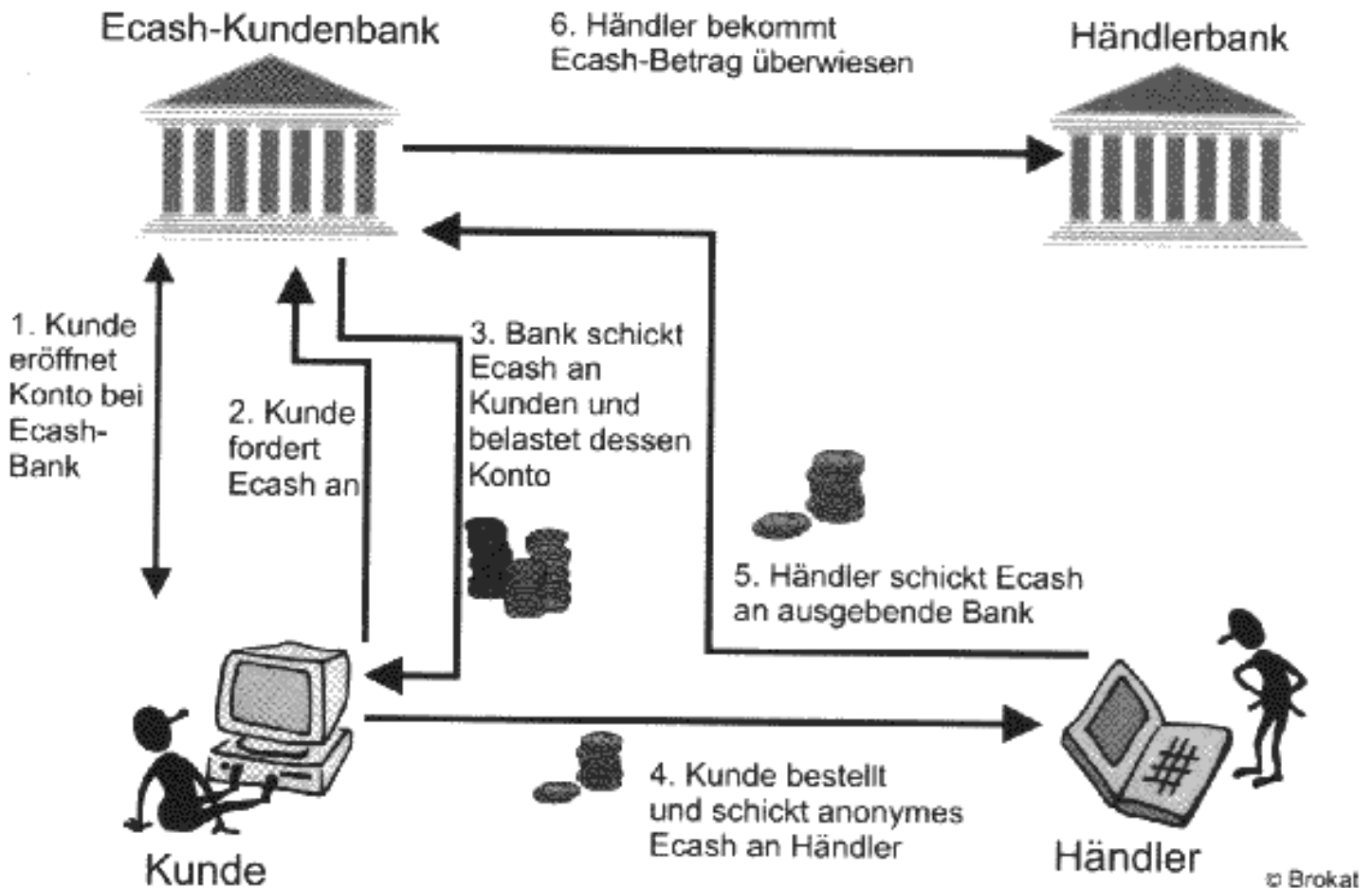


Abbildung 14: Das Online-Zahlungsverfahren von DigiCash

Sollten z.B. durch einen Plattencrash die elektronischen Münzen auf dem PC verloren gehen, können die verlorengegangenen Münzen mit einem Recovery-Mechanismus regeneriert werden. Außerdem sind die eCash-Münzen durch einen Sicherheitsmechanismus gegen Kopieren unbefugter Dritter geschützt [Deutsche 1998].

Das eCash System bietet dem Kunden vollständige Anonymität da es wie Bargeld funktioniert. Teilgenommen haben letztendlich nur 15 Händler. Leider bietet die Deutsche Bank noch keine Informationen über die Ergebnisse des Projektes an.

Inzwischen haben weitere Banken, wie die Dresdner Bank und die Stadtsparkasse Köln, Projekte mit Digitalem Geld angekündigt. Da sich immer mehr bekannte Kreditinstitute als Mittler einschalten und den ordnungsgemäßen Ablauf von Geldtransaktionen garantieren, könnte so mehr Vertrauen für die Online-Bezahlung geschaffen werden. Allerdings ist die Perspektive daß die Großbanken eigene Digital Währungen herausgeben, weniger verlockend. Die Händler und Kunden werden eher auseinander als zusammen

gebracht werden. Und wenn außer den Banken auch andere Einrichtungen digitales Geld "ausstellen" sollten? Wer übt dann die Kontrolle aus? Nach Ansicht der Europäischen Zentralbank (EZB) sollte die Ausgabe des elektronischen Geldes auf Kreditinstitute beschränkt sein.

Die Internet Engineering Task Force (IETF) will Ordnung in die zahlreichen Systeme für Online-Zahlung bringen. Die IETF will das vom Open Trading Protocol Consortium entworfene Internet Open Trading Protocol weiterentwickeln. Dabei soll die Vielzahl existierender Zahlungssysteme wie SET, digitales Geld oder die Geldkarte integriert werden.

8.3 Sicherheit

Frühere Massenmedien wie z.B. das Fernsehen, haben vier wesentliche Eigenschaften, die sie als Null-Risiko-Systeme einstufen:

- Es sind unidirektionale Systeme
- Es sind Systeme die sich von einem ausgehend an viele richten
- Die Identität des Senders ist eindeutig und nicht verdeckt
- Die übertragenen Informationen haben rein passiven Character

Das Internet hat genau die gegenteiligen Eigenschaften:

- Es ist ein bidirektionales System
- Es ist ein System, das sich von vielen an viele richtet
- Die Identität des Informationsversenders ist programmierbar und kann verdeckt werden
- Die übertragenen Informationen können aktive Programme sein

[Schultz 1997, S. 65]

In Deutschland sind die Sicherheitstechnologien noch nicht sehr verbreitet. Einer der Gründe dürfte darin liegen, daß die große Mehrheit der Unternehmen sich im World Wide Web eher passiv präsentiert. Wenn keine Geschäftstransaktionen über das Internet abgewickelt werden, ist die Sicherheit derselben auch kein Thema. E-Commerce erfordert aber Mechanismen die die Vertraulichkeit und Integrität der Transaktion und den beteiligten Partnern garantieren. Die Anforderungen von Händler und Käufer an die Sicherheit von E-Commerce sind naturgemäß verschieden. Für den Händler ist vor allem der rasche, kostengünstige Zahlungseingang von Bedeutung; die Transaktionsdaten müssen fälschungssicher übertragen und die Kreditwürdigkeit bzw. Echtheit des Zahlungsmittels sollte online verifiziert werden können. Für den Kunden hingegen sind Aspekte wie eine einfache Handhabung und der Schutz gegen Mißbrauch und Diebstahl wichtig. Während bei der mißbräuchlichen Verwendung von traditionellen Zahlungsmitteln jeweils ein einzelner, konkreter Mißbrauchsfall vorliegt, erlaubt das Internet jedoch potentiell, zeitgleich sehr viele Informationen (beispielsweise Kreditkarteninformationen) auszuspähen.

Ein Angriff könnte an drei Stellen erfolgen: der Clientrechner, die Übertragung oder der Webserver. Private Informationen könnten auf dem Clientrechner ausgespäht, oder durch fahrlässiges Verhalten seitens des Nutzers einem Angreifer zugänglich gemacht werden. Da das Internet so aufgebaut ist, daß eine Nachricht über verschiedene eingebundene Rechner ihren Weg vom Sender zum Empfänger findet, könnte jeder dieser Rechner die Nachrichten abfangen, kopieren, ändern oder sogar löschen. Webserver die für E-Commerce-Anwendungen eingesetzt werden, werden auch oft zur Speicherung der Kundendaten

genutzt. Nachlässigkeit beim Umgang mit diesen Daten könnte sie für einen potentiellen Angreifer zur leichten Beute machen. Neben den übertragenen Daten und den gespeicherten Daten sollte ganz besonders die Identität der Geschäftspartner geschützt werden. Die folgenden Technologien und Verfahren können eingesetzt werden um diese Daten zu sichern.

8.3.1 Übertragung sichern

Daten können durch Verschlüsseln vor unbefugtem Ausspähen während der Übertragung geschützt werden. Wichtige Sicherheitsaspekte wie der Schutz der Identität der Partner, die Integrität und Authentifizierung der Transaktion und die Sicherstellung, daß nur der gewünschte Empfänger die Nachricht lesen kann, werden von verschiedene Kryptoverfahren unterstützt. Man unterscheidet zwischen der symmetrischen und der asymmetrischen Kryptographie.

8.3.1.1 Symmetrische Kryptographie

Dieses Verfahren wird auch "Private-Key-Chiffrierung" genannt. Der Absender kodiert seine Nachricht mit einem geheimen Schlüssel und macht sie so für Dritte unverständlich. Die Entschlüsselung erfolgt nur unter Verwendung des gleichen Schlüssels. Die Sicherheit dieses Verfahrens resultiert aus dem benutzten Algorithmus und die Länge des Schlüssels. Da für dieses Verfahren ein gemeinsamer Schlüssel zum ver- und entschlüsseln benutzt wird, muß dieser auf einem sicheren Weg zwischen Sender und Empfänger ausgetauscht werden. Wenn es diesen sicheren Weg aber gibt, wieso dann noch verschlüsseln? Man könnte diesen sicheren Kanal doch auch für die Kommunikation nutzen. Dieses Verfahren kann aber auch sinnvollerweise benutzt werden um gespeicherte Daten zu sichern (beispielsweise Archivdateien).

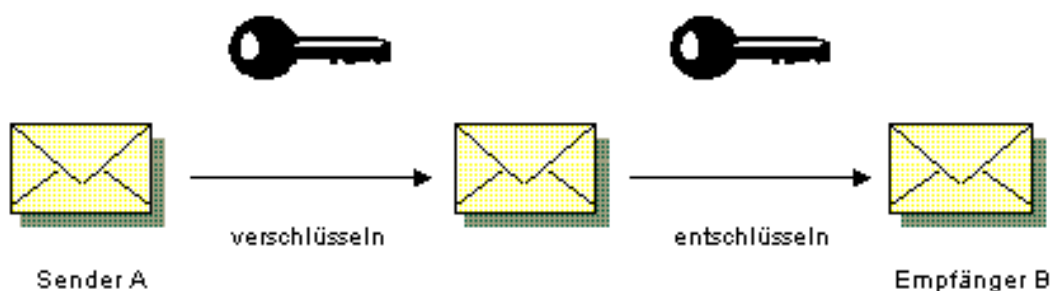


Abbildung 15: Symmetrische Kryptographie

Der Data Encryption Standard (DES) ist das meistverbreitete symmetrische Kryptoverfahren im Internet. Es wurde von IBM entwickelt, ist seit 20 Jahren im Einsatz und wurde 1997 von der amerikanischen Regierung als offizieller Standard propagiert. DES arbeitet mit einem 56 Bit langen Schlüssel. Der Aufwand um einen Schlüssel zu knacken steigt exponentiell mit dessen Länge. Eine Nachricht kann auch mehrmals verschlüsselt werden um die Sicherheit zu steigern. Dreimal verschlüsseln (Triple-DES) verdoppelt die Schlüssellänge effektiv auf 112 Bit und erhöht den Aufwand des Knackers um den Faktor 256 [Dreyer 1998, 6.1.2.3, S. 6]

Allerdings plant das US National Institute of Standards and Technology (NIST) inzwischen die Einführung eines Nachfolgers. Das Advanced Encryption Standard (AES) genannte Verfahren soll neben höherer Sicherheit auch mehr Flexibilität bringen. Geplant sind die Schlüssellängen 128, 192 und 256 Bit. Diverse Firmen, u.a. auch die Deutsche Telekom, haben Vorschläge zu einem möglichen Algorithmus eingereicht. Bis Sommer 1999 sollen dann 5 Systeme ausgewählt werden, aus denen der AES hervorgehen soll [CZ 37 1998, S. 4].

| Angreifer | Budget | Werkzeug | 40 Bit | 56 Bit |
|-----------------|------------------|--|-----------------|-------------|
| Normaler Hacker | Sehr gering | Genutzte Computerzeit an Universitäten oder sonstige Institutionen | Eine Woche | Unmöglich |
| Kleine Firma | Bis 400 \$ | FPGA | Fünf Stunden | 38 Jahre |
| | Bis 10.000 \$ | FPGA | 12 Minuten | 556 Tage |
| Mittlere Firma | 300.000 \$ | FPGA | 24 Sekunden | 19 Tage |
| | | ASIC | 18 Sekunden | 3 Stunden |
| Große Firma | 10 Millionen \$ | FPGA | 7 Sekunden | 13 Stunden |
| | | ASIC | 0.005 Sekunden | 6 Minuten |
| Geheimdienste | 300 Millionen \$ | ASIC | 0.0002 Sekunden | 12 Sekunden |

Tabelle 13: Sicherheit symmetrischer Schlüssel

Die Schlüssellänge sollte nach Art der zu befürchteten Angreifers gewählt werden. Die in Tabelle 13 genannten FPGA- (Field Programmable Gate Array) und ASIC- (Application Specific Integrated Circuit) Chips sind hochleistungs Chips die sich dafür eignen gegen verschiedene Kryptoverfahren eingesetzt zu werden.

8.3.1.2 Asymmetrische Kryptographie

Das Symmetrische Verfahren hat den Nachteil, daß der Sender einer Nachricht erst mal den Schlüssel an den Empfänger schicken muß, und dies über ein sicheres Medium. Asymmetrische Verfahren umgehen dieses Problem. Bei diesen Verfahren, auch Public-Key-Verfahren genannt, werden zwei Schlüssel verwendet: ein Private- und ein Public-Key. Beide werden vom Nutzer erstellt und sind über mathematische Beziehungen verwandt. Der Private-Key wird geheim auf dem Rechner des Nutzers gespeichert. Der Public-Key ist für jedermann zugänglich und kann im Internet auf sogenannten Keyservern abgelegt werden. Der Sender verschlüsselt dann seine Nachrichten mit dem Public-Key des Empfängers. Der Empfänger entschlüsselt die Nachricht mit seinem eigenen geheimen Private-Key, das Gegenstück zu dem zur Verschlüsselung verwendeten Public-Key.

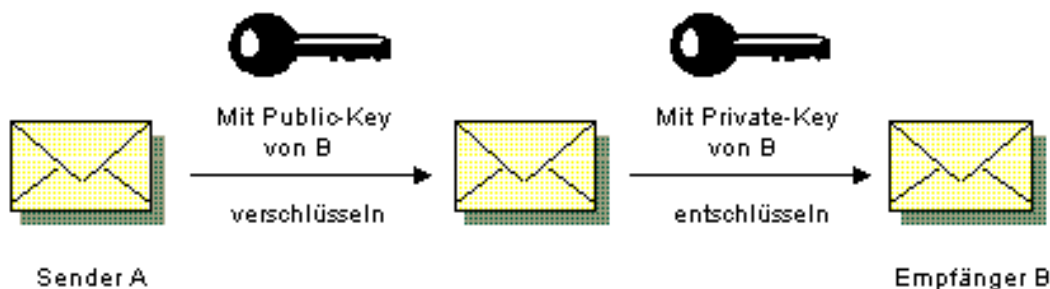


Abbildung 16: Asymmetrische Kryptographie

Auch umgekehrt kann dieses Verfahren eingesetzt werden. Der Sender verschlüsselt seine Nachricht mit seinem Private-Key und der Empfänger entschlüsselt mit dem Public-Key des Senders. Diese

Konstellation wird benutzt um die Authentizität des Senders zu verifizieren.

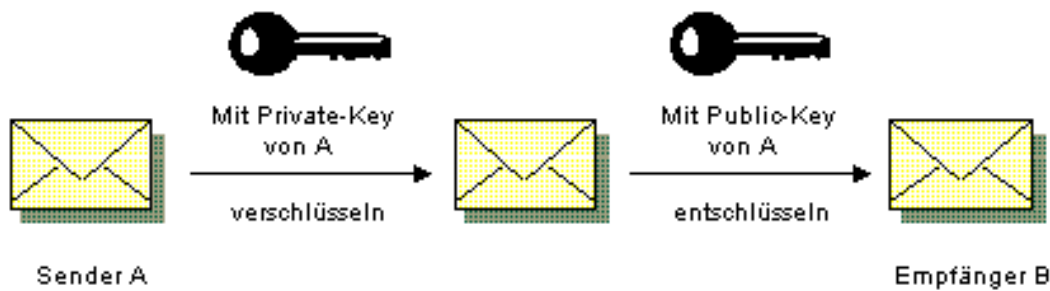


Abbildung 17: Asymmetrische Kryptographie als digitale Unterschrift

Das bekannteste Public-Key-Verfahren heißt RSA nach seinen Erfindern Ron Rivest, Adi Shamir und Leonard Adleman. Da der RSA-Algorithmus zwischen 100 und 1.000 mal langsamer ist als das DES-Verfahren (abhängig von Schlüssellänge), wird oft eine Kombination der beiden benutzt. Zuerst wird der Schlüssel für die symmetrische Verschlüsselung mit dem Public-Key des Empfängers verschlüsselt und verschickt. Dieser entschlüsselt mit seinem Private-Key und die eigentliche Kommunikation wird dann symmetrisch verschlüsselt und ausgetauscht. Die Kombination sorgt daher für eine erhöhte Sicherheit bei der Übertragung des symmetrischen Schlüssels und eine bessere Leistung bei der Übertragung der Nachricht.

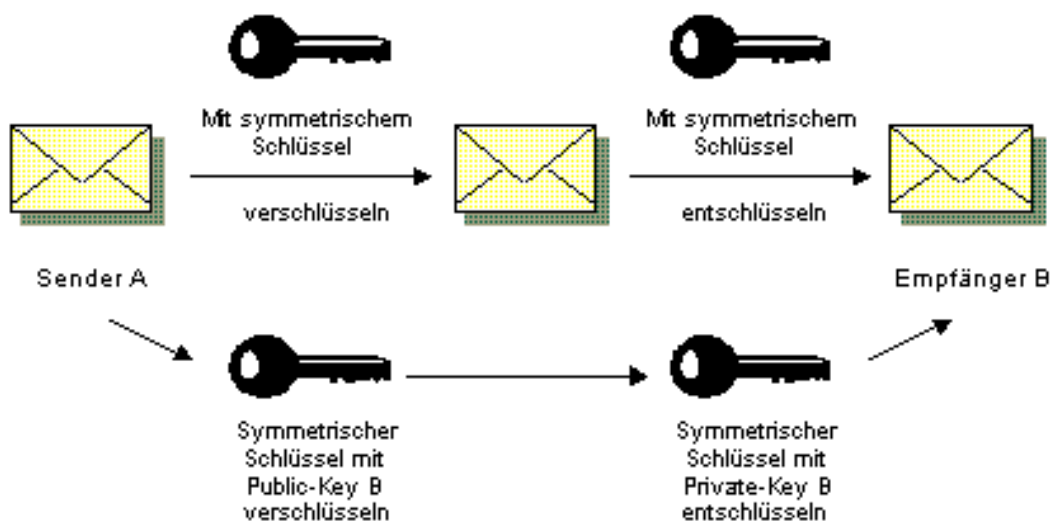


Abbildung 18: Kombination symmetrische/asymmetrische Kryptographie

Pretty Good Privacy (PGP) ist im Internet seit Jahren ein anerkannt sicherer De-Facto-Standard für authentische und vertrauliche Email. PGP wurde in den USA von Philip Zimmermann entwickelt.

"PGP gestattet den Austausch von Nachrichten ohne Verzicht auf Privatsphäre, Authentifikation und Komfort. Hierbei steht Privatsphäre dafür, daß eine Nachricht nur von dem gewünschten Empfänger gelesen werden kann, Authentifikation dafür, daß eine Nachricht überprüfbarerweise von der Person stammt, von der sie zu stammen scheint und Komfort steht dafür, daß der Anwender sich keine unnötigen Gedanken darüber machen muß, wo er welche Schlüssel aufbewahrt und welchen Schlüssel er zum Datenaustausch mit wem benutzt" [Zimmermann 1997, S. 15]

PGP verbindet den schnellen symmetrischen IDEA-Algorithmus (128 Bit Schlüssellänge) mit dem sehr sicheren asymmetrischen RSA-Algorithmus. Das Schlüsselpaar kann eine Länge von wahlweise 384 bis 2048 Bit besitzen. 1024 Bit stellt mit der Rechenleistung aktueller Computer kein Performance-Problem dar und ist mittlerweile Standardwert. Natürlich ist es auch möglich nur symmetrisch zu verschlüsseln. Die

in Abbildung 18 gezeigte Kombination der symmetrischen und asymmetrischen Kryptoverfahren ist ebenso möglich wie auch die folgende Methode. Der Sender verschlüsselt seine Nachricht erst mit dem eigenem Private-Key und dann mit dem Public-Key des Empfängers. Entschlüsselt wird zunächst mit dem Private-Key des Empfängers und dann mit dem Public-Key des Senders. So wird das Briefgeheimnis wie auch die Authentizität des Senders gewährleistet.

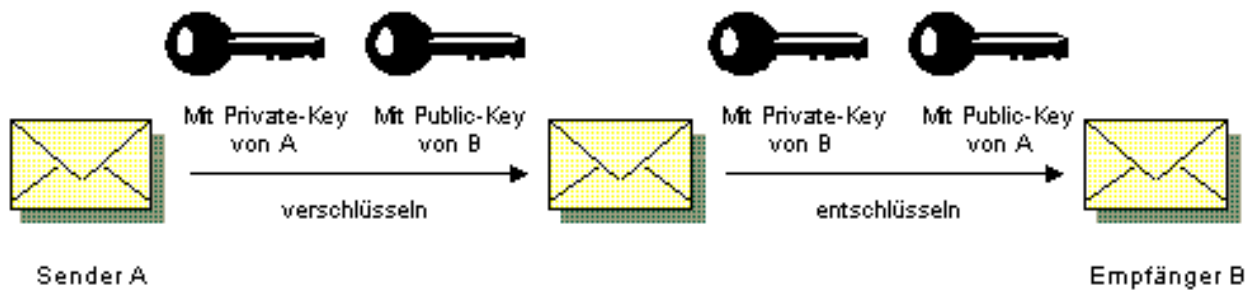


Abbildung 19: Verschlüsselung mit PGP

Die Schlüssel werden durch einen "pass phrase" geschützt. Das entspricht einem beliebig langem Paßwort, auch oft "Mantra" genannt im deutschen. Nur die richtige Eingabe ermöglicht den Zugriff auf die Schlüssel. Diese Maßnahme verhindert das Kopieren oder Ändern der geheimen Schlüssel. Die Public-Keys der Kommunikationspartner werden auf einem "Keyring" (Schlüsselbund) aufgenommen. Dieser Keyring wird in einer Datei auf der Festplatte abgelegt. Vorhandene Schlüssel können gelöscht oder neue aufgenommen werden. PGP betreibt unter www.de.pgp.net/pgp/ einen eigenen Keyserver. Um Nachrichten zu unterschreiben nutzt PGP einen "message digest". Das ist eine Methode um aus einer Nachricht eine 128 Bitzahl als Prüfsumme zu erzeugen, die die Nachricht eindeutig genug bestimmt, daß es praktisch unmöglich ist, die Nachricht zu verändern oder gar neu zu schreiben und die gleiche Prüfsumme zu erhalten. Von der Idee her ist es ähnlich einer Quersumme und repräsentiert eine Art Fingerabdruck der Nachricht. Die 128 Bitzahl wird zusammen mit einer Zeitmarke mit dem Private-Key codiert um eine authentische Unterschrift zu erzeugen und anschließend der Nachricht angehängt. Die Software des Empfängers sucht in seinem Keyring nach dem Schlüssel des Senders und überprüft damit die Unterschrift. Der verwendete Algorithmus ist MD5 (Message Digest 5), 1992 von der RSA Data Security Inc. für die Public-Domain-Verwendung freigegeben. Die Kombination von RSA/IDEA/MD5 ist in der Version 5.0 von der Kombination DH/CAST/SHA-1 ersetzt worden. Allerdings unterstützt es weiterhin die alten Verfahren. Die aktuellste Version ist 6.0 (Stand 08/98), die RSA aber nicht unterstützt.

Der Text in dem oberen Kasten ist im unterem mit PGP verschlüsselt.

Sehr geehrte Damen und Herren,
wie besprochen uebersende ich Ihnen hiermit die neuen Accounts fuer das
Zentralsystem.

Username Passwort

Mueller 4324bhb3

Meier nn33n4jn

Schmidt 424n32

Mit freundlichen Gruessen

```

XXX
-----BEGIN PGP MESSAGE-----
Version: 2.6.3a

hIwD04kTKbrncbOBA/9Wkz/MXQrg9TOHhitoETdLBCcgyP9j+wd+8yg4xaE9zQUY
xnpCTIWY20Zaft2jfWkBvjFacXmeZrStJSR9IIT341Dr9/Qcq9SwlMbiErYWr0xYl
eNFTRwwkAEjbrKXqBaYt76Eymv2Hu3oWwJC7ErtYXLg/FfJF7zIW+VE+mOYTKYA
AADT9fs6UzTzFOye4c0Y6gCZIm5A8r63/lwbzX/UcV7rpEpYGEYoTBIGr46VazX
LLQQOwpZ9SaGpxUgFDdWQp8FuJDTVX/7kkaYOkEZ1BLcv+Q16Jd1AZEiTeHevvPM
82tyDwrmW22l7YXw+fwNyDUshJtAeA02FgbQH1hf+cqiDxdlygZRIHww4PHWInII
B1Efa3Ewj1lBIG7p3maRcfb703186opiccMJs8HV/rlr55dMgCrH94J0y5eZHTpQ
EfmaDnJYog3hsMq+w7qPuVvPl/rnJa==
=MJ31
-----END PGP MESSAGE-----

```

Tabelle 14: Ein mit PGP verschlüsselter Text

Die größte Schwachstelle der asymmetrischen Kryptoverfahren liegt in der Fälschung von Public-Keys. Wenn ein Angreifer seinen Public-Key für den eines anderen ausgibt, kann er als einziger die mit diesem Schlüssel verschlüsselte Nachrichten lesen. Daher sollte der Echtheit von neu erhaltenen Public-Keys nur dann vertraut werden, wenn diese direkt von seinem Besitzer kommt oder wenn die Echtheit von einer vertrauten Person bestätigt wird. Außerdem sollten die Public-Keys auf dem Keyring nur für den Nutzer zugänglich sein. Die Kryptoverfahren sind nicht grundsätzlich unsicher aber dennoch überwindbar.

Die Verbreitung von Kryptoprogrammen bereitet dem Bundesamt für Verfassungsschutz (BfV) große Sorgen. PGP sei in der linksextremistischen Szene jetzt schon eine gebräuchliche Software und in einigen Jahren, wenn Verschlüsselung selbstverständlich ist, wird es von jedem eingesetzt werden. Das BfV befürwortet daher einen Genehmigungsvorbehalt für Kryptoverfahren um die Entschlüsselung "im gesetzlich zulässigen Rahmen sicherzustellen. Die Nutzung ungenehmigter Verfahren sollte gleichzeitig unter Strafe gestellt werden, um eine Beschaffung aus dem Ausland zu vermeiden. Die National Security Agency (NSA) in den USA hat ähnliche Bedenken. Die Hauptaufgabe der NSA ist Aufklärung, hauptsächlich durch das Abhören und Mitlesen von privater Kommunikation. Die NSA hat Unmengen an Wissen und Technik für das Knacken von Verschlüsselungen angesammelt. Wenn die Allgemeinheit keinen Zugang zu guter Kryptotechnik hat, wird die Arbeit der NSA um einiges vereinfacht. Die NSA, wie auch das Federal Bureau of Investigation (FBI), würde es daher gerne sehen wenn sie für jedes Kryptoprogramm einen Generalschlüssel erhielten, um gegebenenfalls codierte Nachrichten knacken zu können. In Deutschland ist das Gegenstück zur NSA der Bundesnachrichtendienst (BND) der seit dem 01. März 1996 alle nötigen Befugnisse hat, um grenzübergreifende Telefonate lückenlos abzuhören. Die Bundesregierung überlegt noch ob und wie die generelle Verschlüsselung reglementiert oder gar verboten werden soll. Zur Diskussion stehen mehrere Ansätze:

- Die Verschlüsselung wird generell verboten
- Es darf nur mit Algorithmen verschlüsselt werden, die staatliche Stellen genehmigt haben. In diese Algorithmen werden bei der Entwicklung "Hintertüren" eingebaut, um Behörden die Entschlüsselung zu ermöglichen⁷.
- Die Länge des Private-Keys wird auf einen Maximalwert begrenzt, um das "Knacken" verschlüsselter Daten auch ohne ihn zu ermöglichen.
- Alle Anwender kryptographischer Techniken werden aufgefordert, Kopien ihrer geheimen

Schlüssel staatlichen stellen zugänglich zu machen [CZ 27 1998, S. 16].

Noch gibt es aber kein Krypto-Gesetz und Wirtschaftsminister Günter Rexrodt bestätigte daß es "keine Nutzungsbeschränkung für Kryptoprodukte in Deutschland" geben werde. Aber je nach Ausgang der Bundestagswahlen könnte die Krypto-Politik im Herbst wieder auf den Tisch kommen [CZ 28 (2) 1998, S. 30].

8.3.1.3 Verschlüsselung in den Internet-Protokollen

Die oben genannten Verschlüsselungsverfahren werden meistens als Zusatzprogramme implementiert. Um sicher miteinander kommunizieren zu können, müssen Sender und Empfänger dasselbe Programm nutzen. Wären die Sicherheitsfunktionen in den Standard Internet-Protokollen integriert, so könnten Kompatibilitätsprobleme, die aufgrund verschiedener Verschlüsselungsprogramme aufkommen, ausgeschlossen werden. Secure-HTTP (S/HTTP) beispielsweise, die Neufassung des HTTP-Protokolls, soll die Sicherheit der Übertragungen im WWW gewährleisten. Noch ist es in der Entwurfsphase. Das W3C versucht die Neufassung mit möglichst vielen und umfassenden Verbesserungen auszustatten. S-HTTP definiert eine spezielle Vorab-Sicherheitsabstimmung. Es wird im Header⁸ definiert, welche Verfahren benutzt werden sollen; die spezifischen Algorithmen die unterstützt werden, die Richtung in der diese Eigenschaften durchgesetzt werden sollen (sendend oder empfangend), und die Art auf der die Eigenschaft eingefordert wird (z.B. obligatorisch oder optional).

Die Netscape Communications Corporation hat die Secure Socket Layer (SSL) entwickelt, eine Zwischenschicht zwischen HTTP und TCP/IP, in die Sicherheitsfunktionen implementiert wurden. Der Vorteil dieses Verfahrens liegt darin, daß es nicht auf HTTP beschränkt ist. Es kann vielmehr für jedes beliebige TCP-basiertes höheres Protokoll (z.B. FTP oder Telnet) genutzt werden. Allerdings ist es zur Zeit nur für HTTP Anwendungen implementiert. Abbildung 20 zeigt die Beziehung zwischen den verschiedenen Protokollen (unter der TCP-Schicht gibt es noch weitere Schicht die hier aber nicht weiter wichtig sind).

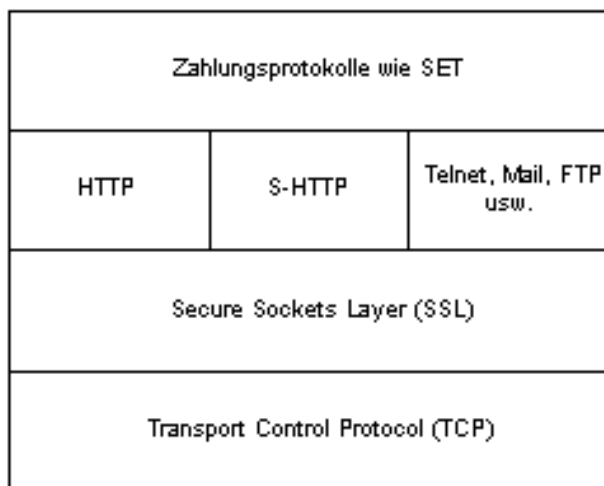


Abbildung 20: Protokoll-Stack für Internet Kommunikation

SSL gewährleistet die sichere Kommunikation, die Authentifizierung der Partner und die Integrität der übertragenen Daten. Das vorgenannte Public-Key-Verfahren wird benutzt, um beide Partner zu authentifizieren und um einen Private-Key auszutauschen. Die Daten werden dann mit diesem Schlüssel symmetrisch verschlüsselt und verschickt. Auch hier wird die Kombination beider Kryptoverfahren aus Performancegründen benutzt.

Wenn eine sichere Übertragung initiiert werden soll, schickt der Client ein "Client Hallo" an den Server. Dieses "Hallo" besteht aus einer Zusammenstellung von sicheren Protokollen die der Browser des Clients unterstützt und eine zufällig generierte Zeichenkette. Der Server antwortet mit einem "Server Hallo" und der Bestätigung daß einer dieser Protokollen auch von dem Browser des Servers unterstützt wird. Das "Server Hallo" beinhaltet seine Zertifizierung und eine Zufalls-Verbindungs-ID. Der Client Browser prüft dann die digitale Signatur des Servers mit Hilfe der ausstellenden Zertifizierungsstelle. Als nächstes generiert der Client Browser einen symmetrischen "Master-Key" (Sitzungsschlüssel) der nur zwischen Client und Server ausgetauscht wird (da der Client Browser diesen generiert, ist es ausgeschlossen, daß ein Server den gleichen Schlüssel mehrmals verwenden kann). Dieser Master-Key wird mit dem Public-Key des Servers verschlüsselt und verschickt. Er wird benutzt um symmetrische Schlüssel für die Datenübertragung zu generieren. Ab diesem Punkt kommt auch nur noch die symmetrische Verschlüsselung zum Einsatz. Der Client verschlüsselt die erhaltene Verbindungs-ID und schickt diese zum Server. Wenn diese die gleiche ist die er zu Beginn verschickte, dann kann er sie auch entschlüsseln. Daraufhin verschlüsselt der Server die zufällig generierte Zeichenkette des Clients und schickt sie zurück zum Client. Wenn der Vergleich der entschlüsselten Zeichenkette und die zuvor gesendete positiv ausfällt, so ist eine sichere Verbindung aufgebaut worden. Jetzt beginnt die eigentliche Datenübertragung. Optional ist natürlich auch eine Authentifizierung des Clients möglich.

Da die Masterkeys zufällig generiert werden, kann deren Verlust nicht die Sicherheit anderer Sitzungen kompromittieren. Allerdings darf Netscape, um die Exportlizenz zu erhalten, nur 40 Bit lange Schlüssel generieren. Zur Nutzung des Verfahrens sind allerdings spezielle Clients und Server notwendig die SSL beherrschen.

Eine Nachricht im Internet zu verschicken kann mit dem Versand einer Postkarte verglichen werden. Deswegen sollte eine unverschlüsselte Nachricht nie etwas enthalten was nicht auch auf einer Postkarte stehen könnte. Ein Gegner könnte mühelos (sogar routinemäßig) die Datenkommunikation abfangen.

"Verwenden Sie deshalb immer einen elektronischen Briefumschlag zur Wahrung der Fernmeldegeheimnisses" [Zimmermann 1997, S. 7].

8.3.2 Webserver sichern

Die Übertragung der Daten kann also relativ gut gesichert werden. Aber was bringt der beste Übertragungsschutz, wenn die übertragenen Daten letztendlich auf einem Webserver gespeichert werden, der nicht so halb so gut oder sogar gar nicht gesichert ist. In der Regel suchen sich Angreifer das schwächste Glied einer Kette für ihren Angriff aus.

Wird ein Webserver angegriffen und die Seiten vandalisiert, entsteht für das Unternehmen ein Image Verlust. Im September 1996 wurde die Website der [CIA](#) in den USA angegriffen. Die geschädigte Seite erhielt die Überschrift "Welcome to the Central Stupidity Agency" und enthielt u.a. Links zur Playboy Website und zu verschiedenen Hacker-Websites. Und sogar noch im März 1997 wurde die Website der [NASA](#) Ziel eines solchen Angriffs.

Einige der Maßnahmen die die Gefahren verringern werden nachfolgend vorgestellt. Die Option "Automatic directory listing" ist meistens defaultmäßig angeschaltet. Wird eine Webadresse wie [www.firma.de](#) (ohne Angabe eines bestimmten Dateinamens) angesteuert, so sind die meisten Server so eingestellt, daß sie daraufhin automatisch eine Datei, die "index.html" heißt, an den Nutzer schicken. Ist

die Option "Automatic directory listing" aber an und existiert keine "index.html"-Datei, so wird das Inhaltsverzeichnis des Servers angezeigt. Der Nutzer kann jede Datei in diesem Verzeichnis auf seinem Rechner kopieren, eventuelle CGI Programme studieren um mögliche Lücken aufzuspüren und auszunutzen. Die Option sollte daher ausgeschaltet sein oder jedes anwählbares Verzeichnis müßte eine index.html besitzen. Außerdem sollte der Server so konfiguriert werden, daß er nur Dateien ausliefert, die in einem bestimmten Verzeichnis mit einer bestimmten Endung (z.B. ".html") abgelegt sind und auf gar keinen Fall Systemdateien.

Als nächstes kann der Zugang zum Webserver auf autorisierte Personen beschränkt werden. Jedem Aufruf einer Webseite werden die Angaben zum Host des Nutzers und seine IP-Adresse beigefügt. Auf dieser Basis kann schon eine Zugangskontrolle aufgebaut werden. Der Webserver kann anhand des Domain Name Systems⁹ (DNS) prüfen, ob der Hostname mit der IP-Adresse übereinstimmt. In einem "double-reverse look-up" holt sich der Server erst den zugehörigen Domainnamen zu der geschickten IP-Adresse. Dann holt der Server die IP-Adresse, die dem ermittelten Domainnamen zugeordnet ist. Wenn diese IP-Adresse nicht mit der geschickten übereinstimmt, wird die Verbindung beendet. Zusätzlich kann jetzt anhand von Zugangskontrolllisten geprüft werden, ob diese IP-Adresse berechtigt ist die aufgerufene Seite zu besichtigen.

Dann ermöglicht eine Paßwortabfrage eine weitere Einschränkung der Nutzer die eine Webseite aufrufen. Eine Möglichkeit ist "Basic Authentication". Wenn ein Client auf ein so geschütztes Dokument zugreift, verweigert der Server die Auslieferung bis der Client eine gültige Nutzer-ID und ein Paßwort eingibt. Natürlich können auch eigene Abfragen entwickelt werden. Basic Authentication verschickt die Daten nämlich nur in einem Format, daß sehr einfach zu "entschlüsseln" ist. Eigene Berechtigungsabfragen sollten daher eine Verschlüsselung der übertragenden Daten einbinden. Für die Paßwortabfrage muß der Server-Administrator eine Datenbank der berechtigten Nutzer mit ihren Nutzer-ID's und Paßwörtern einrichten. Die Paßwörter sollten nur verschlüsselt abgelegt werden. Ein weiteres Sicherheitsrisiko liegt in der Wahl der Paßwörter. Da die Nutzer in der Regel ihre Paßwörter selber wählen muß gewährleisten werden, daß diese nicht leicht zu erraten sind. Leicht zu erratende Paßwörter sind beispielsweise die Namen von Kindern, Partnern oder Haustieren. Mit nur einem geknacktem Paßwort kann die Sicherheit des gesamten Systems kompromittiert werden. Zusätzlich muß der Administrator festlegen, welche Bereiche auf dieser Weise zu schützen sind.

Eine weitere Absicherung ist die Authentifikation der Partner. Das SSL¹⁰ kann so konfiguriert werden, daß es entweder eine Partei authentifiziert oder gleich beide.

Einige Server speichern die Zugangsdaten eines Nutzers auf seinem Rechner mit Hilfe von Cookies. Wenn der Nutzer den Server ein weiteres Mal anwählt, liest dieser die Daten aus dem Cookie und ermittelt so die Berechtigung. Damit wird dem Nutzer erspart sich jedesmal neu anmelden zu müssen. Diese Daten können während der Übertragung abgefangen werden, sofern diese nicht verschlüsselt erfolgt oder vom Rechner des Nutzers kopiert werden. Zugangsdaten für sicherheitskritische Bereiche sollten daher nicht in Cookies gespeichert werden sondern nur auf dem Webserver selbst.

Programme, die auf dem Server abgearbeitet werden, wie beispielsweise CGI-Skripte oder Server-Side Includes wie Server-side JavaScript, sind besonders fehleranfällig. Diese Programme besitzen grundsätzlich die Fähigkeit, Dateien auf dem Server zu lesen und schreiben und außerdem Programme auf dem Server auszuführen. Beim Verschicken von Online-Formularen könnten zum Beispiel anstelle der normalen Feldinhalte ganz andere Zeichenfolgen verschickt werden. Daher sollte in der Implementierung solcher Formulare eine Prüfung auf Anzahl und Inhalt der Felder vorgesehen sein. So sollten auch

Dateinamen, auf die zugegriffen werden soll, nicht aufgrund von Benutzereingaben festgelegt werden.

Zuletzt kann eine Firewall zwischen den kritischen Sicherheitsdaten und dem Internet geschaltet werden. Es fungiert dabei als Schranke oder elektronischer Pförtner, so daß jeglicher Datenverkehr von und zum Internet nur über das Firewall-System möglich ist. Eine Firewall stellt einen Kompromiß dar zwischen dem Lösen der Verbindung zum Internet und der völligen Freigabe aller Rechner. Im Folgenden werden die Ziele eines Firewall-Systems so wie sie in [Dreyer 1998, 6.3, S. 2 f] beschrieben sind, aufgelistet.

- **Zugangskontrolle auf Netzwerkebene:**
Hier wird überprüft, welche Rechnersysteme über die Firewall miteinander kommunizieren dürfen.
- **Zugangskontrolle auf Netzwerkebene:**
Das Firewall-System überprüft, welche Benutzer über die Firewall eine Kommunikation aufbauen dürfen. Dazu wird die Authentizität des Benutzers festgestellt.
- **Rechteverwaltung:**
Im Rahmen der Rechteverwaltung wird festgelegt, mit welchen Protokollen und Diensten und zu welchen Zeiten über das Firewall-System eine Kommunikation stattfinden darf.
- **Kontrolle auf der Anwendungsebene:**
Es wird überprüft, ob Kommandos genutzt oder Dateiinhalte übertragen werden, die nicht zur durch die Anwendung definierten Aufgabenstellung gehören.
- **Entkopplung von Diensten:**
Dienste werden entkoppelt, damit Implementierungsfehler, Schwachstellen und Konzeptionsfehler der Dienste nicht die Möglichkeit für Angriffe bieten.
- **Beweissicherung und Protokollauswertung:**
Verbindungsdaten und sicherheitsrelevante Ereignisse werden protokolliert und können für die Beweissicherung von Handlungen der Benutzer und für die Erkennung von Sicherheitsverletzungen ausgewertet werden.
- **Alarmierung:**
Besonders sicherheitsrelevante Ereignisse werden an ein Security Management gesendet, damit schnell reagiert werden kann.
- **Verbergen der internen Netzstruktur:**
Ziel ist es, die Struktur des zu schützenden Netzes gegenüber dem unsicheren Netz zu verbergen. Aus dem unsicheren Netz soll nicht sichtbar sein, ob im zu schützenden Netz 10, 100, 1.000 oder 10.000 Rechnersysteme vorhanden sind.
- **Vertraulichkeit der Nachrichten:**
Nachrichten können nicht im Klartext gelesen werden. Dadurch ist die Vertraulichkeit der Daten bei einer Übertragung über unsichere Netze gewährleistet. Ein weiteres Ziel ist es das Firewall-System selbst gegen Angriffe zu schützen. Der Netz Administrator muß außerdem davon ausgehen, daß immer wieder Sicherheitslücken in allen Komponenten (z.B. Server-Software) entdeckt werden können und dann entsprechende Gegenmaßnahmen (z.B. Patches) treffen.

8.3.3 Clientrechner sichern

Neben dem Webserver ist auch die Internet-Software des Nutzers ein wunder Punkt. Da ein Online-Anbieter kein Einfluß auf die eingesetzte Software der Nutzer nehmen kann, werden mögliche Gefahren hier nur kurz aufgezählt.

Bevor es "active content" gab, waren Webseiten statische Darstellungen von Information so ähnlich wie Plakatwände. Mit "active content" werden Programme bezeichnet die in HTML-Seiten

eingebunden werden um Interaktion mit den Nutzern zu ermöglichen. Diese Programme existieren in viele Formen. ActiveX Controls, Java Applets, Skriptsprachen wie JavaScript und VBScript gelten alle als Active content. Auch Graphiken und Videos können als Active content klassifiziert werden, da die dazugehörigen Plug-ins die Anweisungen in den Bilddateien ausführen. Relativ neu gehört auch die Push-Technologie zu den Active content. Die Push-Technology ist die Umkehrung des Normalfalls, daß der Nutzer Informationen aktiv abrufen. Hier legt der Nutzer fest, welche Informationen ihn interessieren und wie oft diese aktualisiert werden sollen. Dann schiebt ("push") der Webserver die gewünschten Informationen in den festgelegten Intervallen auf den Rechner des Nutzers.

Obwohl Active content durchaus gute Seiten hat (so werden zum Beispiel Spiele, Rätsel, usw. damit implementiert) kann es aber auch genutzt werden, um versteckte Prozesse auf dem Rechner des Nutzers ablaufen zu lassen. Ein ActiveX-Control beispielsweise kann jedes Programm ausführen, das auch ein Windows-Programm starten kann. Das hat u.a. der Chaos Computer Club (CCC) im Januar 1997 bewiesen als er mit einem ActiveX-Control auf einer Website das Finanzprogramm Quicken auf den Rechnern der Nutzer startete und Überweisungen tätigte. Eine Sicherheitslücke im Internet Explorer 3.x und 4.0, die im August 1997 entdeckt wurde, erlaubt es einem Java-Applet, eine Netzverbindung zu einem anderen Server als dem, von dem es geladen wurde, aufzubauen. So könnten eingegebene Daten des Nutzers zum Beispiel an einen anderen Server weitergeleitet werden. Auch JavaScript besitzt in den Versionen 2.x, 3.x und 4.0 des Netscape Navigators und 3.x und 4.0 des Internet Explorers eine Lücke, mit dem es potentiell möglich wäre zu dokumentieren, auf welchen Servern der Nutzer weitersurft und welche Daten er in eventuelle Formulare einträgt.

Leider sind auch die Browser selbst potentielle Gefahrenquellen. Eine dänische Firma hat zum Beispiel ein Sicherheitsloch im Netscape Navigator (2.x, 3.x und 4.x) gefunden, mit dem die lokalen Dateien angezeigt werden können auch dann wenn sich der Rechner hinter einer Firewall befindet.

Natürlich sind die Softwarehersteller bemüht, solche Sicherheitslöcher schnellsten zu stopfen. Der beste Rat ist und bleibt: Active content nur von vertrauenswürdigen Websites auszuführen [Ghosh 1998, S.31 ff].

8.4 Technik

Über die normale analoge Telefonleitung ist eine Übertragungsrate von 56 000 Bit pro Sekunde möglich. Mit ISDN sind bereits 128 000 Bit pro Sekunde erreichbar, wenn beide ISDN-Leitungen belegt werden. Allerdings verdoppeln sich auch die Telefonkosten und man ist telefonisch nicht erreichbar. Um die Geschwindigkeit zu erhöhen waren Glasfaserkabel vorgesehen. Diese ermöglichen eine Übertragungsrate von 155 000 000 Bit pro Sekunde (155 Megabit). Das entspricht der Übertragung einer ganzen Enzyklopädie in einer einzigen Sekunde. Allerdings sind die Kosten für die neue Leitungen sehr hoch.

Die neue Technik ADSL ("Asymmetric Digital Subscriber Line) schafft zwar "nur" 3 000 000 Bit pro Sekunde (3 Megabit), nutzt aber die vorhandenen herkömmlichen Leitungen. ADSL ersetzt nicht die vorhanden analogen oder digitalen Techniken, sondern es ergänzt sie. Ein ADSL-Modem entspricht eher einem Netzwerk-Adapter, der die Entfernung vom Nutzer zum Provider überbrückt, als einem Modem. ADSL-Modems formen die Daten statt in nur wenige hörbare Töne (wie beim

normalen Modem) in viele verschiedene gleichzeitig übertragene hohe (für Menschen unhörbare) Frequenzen um. Da diese Frequenzen oberhalb des Hörbereichs liegen, wird der normale Telefonbetrieb nicht gestört. Die Technik heißt "asymmetrisch", da die Downstream-Richtung schneller ausgelegt ist als die Upstream-Richtung.

Die Telekom testet ADSL seit November 1997 in einem Pilotprojekt zusammen mit Siemens und Studenten der Universität Münster. Da werden u.a. Vorlesungen mit einer konventionellen Kamera aufgezeichnet und zum Download angeboten. Im Juni 1998 startete ein neues Pilotprojekt für ca. 450 T-Online-Kunden in Dortmund, Köln, Bonn und Düsseldorf. Bis ins Jahr 2003 will die Telekom ihr Angebot auf 70 Ortsnetze ausdehnen. Je nach Entfernung von der Vermittlungsstelle erreicht ADSL beim Geschäftskundenanschluß theoretisch eine Übertragungsrate von 8 Megabit pro Sekunde downstream, also vom Internet zum ADSL-Modem. In der Gegenrichtung sind maximal 768 000 pro Sekunde möglich. Die Übertragungsrate hängt außerdem noch davon ab ob der genutzte Anschluß analog oder digital ist. Privatkunden wird der Anschluß mit nur 1,5 Megabit downstream und 128 000 Bit upstream angeboten (aber dafür billiger). Dieses "ADSL-Lite", auch UDSL (Universal Digital Subscriber Line) genannt, ist ein abgespeckter Standard, der von der Universal ADSL Working Group, zu der u.a. die Telekom, die France Telecom und British Telecommunications gehören, entwickelt worden. Er soll die Kompatibilität der Hardware sicherstellen und helfen, die Kosten für Installation und Endgeräte zu verringern.

Neben ADSL-Modems könnten Kabelmodems den Internet-Zugang beschleunigen. Sie übertragen über das Fernsehnetz je nach Bauart bis zu 40 Megabit pro Sekunde. In den USA bieten schon einige Kabelgesellschaften Internet über Fernsehkabel an. Beide Technologien haben das Ziel, über ein vorhandenes Medium und zusätzlich zur schon existierenden Nutzung breitbandig Daten zu übertragen. Bei ADSL wird jeder Anschluß einzeln versorgt. Die nutzbare Übertragungsrate ist daher für den Anwender identisch mit der maximal möglichen Geschwindigkeit. Sicherheits- bzw. Zugriffsprobleme sind geringer, da jeder Anwender individuell über sein "eigenes" Kabel angeschlossen ist. Demgegenüber glänzt das Kabelmodem mit extrem hohen Übertragungsraten. Diese können aber in Abhängigkeit vom Nutzverhalten wegen des Shared-Medium-Charakters sehr schnell in den Keller gehen. In Deutschland gibt die Telekom deshalb insbesondere der ADSL-Technik den Vorzug [c't 13/97, S. 164].

Zusätzlich ist die drahtlose Übertragung über Satelliten möglich und auch schon im Einsatz. Das System ist asymmetrisch. Der Nutzer verschickt seine Anfragen upstream über ein normales Modem an das Network Operations Centre (NOC) und empfängt die angeforderten Daten downstream mit 400 000 Bit pro Sekunde via Satellit. Um dieses System zu nutzen, benötigt der Teilnehmer einen PCI Adapter und eine 60-80 cm Schüsselantenne. Der Teilnehmer empfängt die Satellitensignale über die Schüsselantenne die an seinen PC angeschlossen ist. Die Datenpakete werden DES-verschlüsselt¹¹. Diese Lösung wird in Deutschland von [DirecPC](#) über Eutelsat II F3 auf 16 Grad Ost auch schon angeboten.

8.5 Certification Authority

Certification Authorities (CA) sind Zertifizierungsstellen für das Internet. Sie erlauben zwei Parteien, die ein Geschäft übers Internet abwickeln möchten, die gegenseitig angegebene Identität zu vertrauen.

Neben der Verschlüsselung spielt die digitale Signatur für die fälschungs- und manipulationssichere Datenübertragung eine wichtige Rolle. Der Austausch von Public-Keys genügt nämlich nicht um die Identität des Partners zweifelsfrei festzustellen.

Am Jahresende wird die gesetzeskonforme digitale Signatur¹² in Deutschland zum Einsatz kommen. Die Zuverlässigkeit und Integrität der CAs muß wiederum von einem weiteren Zertifizierer gewährleistet werden. Im September 1998 wird die Regulierungsbehörde für Post und Telekommunikation die ersten Zertifizierungsstellen für digitale Signaturen nach dem Signaturgesetz genehmigen. Als zuständige Bundesbehörde kontrolliert und beglaubigt sie die privaten und öffentlichen Zertifizierungsstellen. Zwanzig Anbieter, darunter Telesec der Deutschen Telekom und Debis Systemhaus Information Security Services, warten auf die offizielle Zulassung. Dadurch werden sie zu vertrauenswürdigen Instanzen für Anbieter und Anwender. Primär stellt eine Zertifizierungsstelle die Identität beider Seiten fest. Dazu müßte ein Privatanwender einen Antrag auf die digitale Signatur stellen in dem er Personalien wie Name, Geburtsdatum und Wohnort angibt. Für Geschäftskunden könnte eine Überprüfung über Auskunftsteile vorgesehen werden. Die CA errechnet dann ein Schlüsselpaar für den Nutzer. Alternativ kann der Nutzer auch mit Krypto-Software wie PGP ein eigenes Schlüsselpaar erstellen. Die CA signiert daraufhin die Personalien und den Public-Key mit einem eigenen Schlüssel, dem Zertifikat. Der Private-Key wird auf einer Chipkarte gespeichert und ist nicht auslesbar. Die notwendigen Programme und Chipkarten werden von den Zertifizierungsstellen ausgegeben. Da das Signaturgesetz zwingend eine Chipkarte mit Krypto-Chip vorschreibt, werden deutsche Gerichte die digitalen Signaturen von Kryptoverfahren wie PGP¹³ nicht anerkennen. Noch werden die neuen Signaturen nur hierzulande anerkannt, internationale Vereinbarungen müssen für einen weltweit rechtssicheren Datenaustausch noch ausgehandelt werden.

Die digitale Signatur kann praktisch an jedem Computer, der mit einem entsprechenden Chipkartenleser und der nötigen Software ausgestattet ist, geleistet werden. So auch beispielsweise als dokumentenechter Nachweis für Behörden etwa bei einer Anmeldung in einer neuen Gemeinde.

Der Gesetzgeber sieht für die Zertifizierer ein zweistufiges Modell vor: Hinter den kommerziellen und öffentlichen Zertifizierern steht einzig und allein die Regulierungsbehörde. Sie hält die Public-Keys bereit, mit denen die Zertifikate der CAs überprüft werden können. Das deutsche Gesetz für die Zertifizierung und digitale Signatur gilt derzeit als das ausgereifteste in Europa.

Zertifizierungsstellen bilden heute eine junge und dynamische Dienstleistungsbranche. Sie repräsentieren Vertrauensstellen für beide Partner eines Kommunikationsvorganges. Eine weitere mögliche Aufgabe für CAs wäre das Zertifizieren von E-Commerce Software und Technologien. In den vorigen Kapiteln ist klar zu erkennen, daß eine Menge Protokolle für die Online-Zahlung und die sichere Übertragung existieren. Nutzer können heute wählen zwischen SSL, S-HTTP, SET, CyberCash, FirstVirtual, DigiCash usw. Da diese Verfahren untereinander oft inkompatibel sind, müssen sich die Nutzer für eines entscheiden. Eigentlich trifft der Händler diese Wahl indem er sich für ein Verfahren entscheidet in der Hoffnung, daß sich dieses Verfahren durchsetzt und seine potentielle Kunden es auch unterstützen. Eine offizielle Zertifizierung der Kompatibilität dieser Produkte könnte die Hersteller anregen, offene Schnittstellen zu implementieren. Darüberhinaus könnte eine Zertifizierung der Sicherheit eine Transparenz für die Nutzer schaffen und die Hersteller frühzeitig auf Sicherheitslücken hinweisen (bevor ein Schaden durch Hacker angerichtet werden kann).

Wenn sich E-Commerce weiter ausbreitet, wird die Certification Authority Branche sehr an Einfluß gewinnen.

¹Ein Softwareagent ist ein ereignisgesteuertes Programm

²Siehe auch [Abschnitt 8.3.1 Übertragung sichern](#)

³Unter <http://www.annonce.de> können die aktuellen Anzeigen im Abonnement für fünf Mark monatlich gelesen werden

⁴Siehe auch [Abschnitt 5.4.1 Vertragsrecht](#)

⁵Smartcards ist der Oberbegriff für Chipkarten wie eine EC-Karte oder Telefonkarte.

⁶siehe auch [Abschnitt 8.3.1 Übertragung sichern](#)

⁷1993 stellte die US-Regierung ein Konzept vor, bei dem ein Chip namens "Clipper" in jedes Kommunikationsgerät, sprich Telefon, Faxgerät usw. eingebaut werden sollte. Jeder Chip sollte einen individuellen Schlüssel bekommen von dem die Regierung eine Kopie besaß. Nach massiven Protesten scheiterte das Projekt.

⁸Kopfteil einer Nachricht

⁹Das Domain Name System ermöglicht es, einen Domänenamen in die dazugehörige IP-Adresse umzuschlüsseln.

¹⁰Siehe auch [Abschnitt 8.3.1.3 Verschlüsselung in den Internet-Protokollen](#)

¹¹Siehe auch [Abschnitt 8.3.1.1 Symmetrische Kryptographie](#)

¹²Siehe auch [Abschnitt 5.4.1 Vertragsrecht](#)

¹³Siehe auch [Abschnitt 8.3.1.2 Asymmetrische Kryptographie](#)

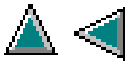




Kapitel 9: SCHLUßWORT

Das Internet in seiner heutigen Form wurde von engagierten Menschen aus vielen Ländern und Kontinenten errichtet, die den Glauben daran teilten, daß die Kommunikation in einem offenen Netz zwischen allen Teilnehmern ungehindert und über alle Grenzen hinweg stattfinden und vorhandene Informationen weltweit frei zur Verfügung stehen sollten. Dieses Erbe darf bei der weiteren Entwicklung des Netzes trotz der zur Bewältigung der anstehenden Probleme möglicherweise erforderlichen Kommerzialisierung nicht verspielt werden. [Krüger 1998]





ANHANG

[Anhang A Quellcode](#)

[Anhang B Cookies](#)

[Anhang C Literaturverzeichnis](#)

[Anhang D Websites](#)

[Anhang E Abkürzungsverzeichnis](#)

[Anhang F Tabellen- und Abbildungsverzeichnis](#)

[Anhang G Glossar](#)

A Quellcode

Die Website ist unter www.kohlhage.de in Kürze aufrufbar.

B Cookies

Cookies sind kleine elektronische "Krümel", die es dem Server, mit Hilfe des Browsers, ermöglichen, Informationen auf der Festplatte des Surfers abzulegen. Sie werden verglichen mit den Coupons die man bei einer Reinigung bekommt. Wenn man die Reinigung wieder aufsucht wird das Gegenstück dazu gesucht, um die dazugehörenden Sachen zu finden. Klassische Anwendungen sind:

- Online Bestellsysteme: hier werden Cookies benutzt um den Inhalt des Warenkorbs festzuhalten. Möglich ist es auch, den Inhalt bis zum nächsten Besuch des Surfers festzuhalten.
- Mass Customization: Cookies werden hier benutzt um die vielen Surfer individuell zu behandeln. Die Interessen eines Surfers werden einmal festgehalten. Jedes weitere Mal wenn er die Site betritt wird diese nach seinen Wünschen konfiguriert. Ein Beispiel wäre eine Nachrichten-Website. Der Surfer kann einstellen, daß er sich nur für Sportnachrichten interessiert und nur diese werden dann auch angezeigt. Er muß sich nicht jedesmal mühsam durchklicken.
- Website Tracking: Anbieter von Websites benutzen Cookies um zu protokollieren welche Seiten ihres Angebots die Surfer besuchen und von welchen Seiten aus sie die Site wieder verlassen.
- Gezieltes Marketing: Cookies werden außerdem noch benutzt um festzuhalten welche Werbeanzeigen vom einem Surfer verfolgt werden. Dann werden gezielt Banner nach seinem Interessensgebiet angezeigt. [Cookie 1998]

Ein non-persistent Cookie wird zur Laufzeit im Arbeitsspeicher des Clients gehalten und beim Verlassen der Site automatisch gelöscht. Persistente Cookies werden mit einem Ablaufdatum versehen und werden nach Verlassen der Site auf die Festplatte des Surfers gespeichert (mit dem Netscape Browser wäre das in die Datei cookie.txt). Pro Domäne dürfen 20 Cookies à 4 Kbyte gespeichert werden.

Ein Cookie unterliegt den folgenden Einschränkungen:

- Er kann nicht ausgeführt werden. Seine Inhalte können nur von einer HTML-Seite ausgelesen werden.
- Er kann nur von der Domäne gelesen werden, die ihn auch gesetzt hat. Zusätzlich kann beim Schreiben von Cookies angegeben werden, welche weiteren URLs auf den Cookie zugreifen dürfen.
- Er kann nicht benutzt werden um Daten auf der Festplatte des Surfers auszuspionieren oder auch um seine E-Mail Adresse oder Identität weiterzugeben.

Die Browser¹ erlauben folgende Einstellungen bezüglich der Cookies:

- Grundsätzlich alle Cookies zu akzeptieren ohne Benachrichtigung
- Alle Cookies zu akzeptieren, die vom ursprünglich sendenden Server kommen
- Warnung bevor ein Cookie auf die Festplatte geschrieben wird
- Grundsätzlich alle Cookies abzulehnen ohne Benachrichtigung.

Die Cookies werden zeilenweise pro Domäne gespeichert. Die einzelnen Werte werden mit Tabs getrennt. Nachfolgend ein Beispiel aus der Cookie.txt eines Netscape Browsers:

```
.netscape.com TRUE / FALSE 946684799 NETSCAPE_ID 100103
```

Die erste Angabe ist der Name der Domäne die den Cookie gesetzt hat. Das "TRUE" legt fest, daß nur Dateien von dieser Domäne den Cookie bearbeiten dürfen. Als nächstes wird ein Pfad angegeben der auf den Cookie zugreifen kann. In dem Beispiel "/" sind es alle Dateien der Domäne. Die "FALSE" Angabe steht für die Notwendigkeit einer gesicherten Übertragung. Die darauffolgende Nummer ist das Ablaufdatum des Cookies. Dann folgen Name und Wert des Cookies.

Die Firma Doubleclick in New York hat sich auf Webbasierte Werbung spezialisiert. Cookies bilden die Grundlage ihrer Maßnahmen um Werbung gezielt einsetzen und detaillierte Analysen erarbeiten zu können.

DoubleClick fügt Werbeanzeigen von ihrem Server auf HTML-Seiten von rund 60 verbündeten Websites ein. Jedesmal wenn ein Surfer einer dieser Seiten lädt, baut der Browser kurz eine Verbindung zum Doubleclick Server auf, um eine Anzeige zu holen. Kurz darauf wird eine eindeutige ID vergeben und in einem Cookie auf der Festplatte des Surfers gespeichert. Gleichzeitig wird ein neuer Datensatz in der Datenbank von Doubleclick erstellt der die schon

gezeigten Werbefbanner festhält.

Der gesetzte Cookie wird als Index zur Datenbank genutzt. Gespeichert werden der Browsertyp, Betriebssystem, die Domäne und andere verwandte Informationen. Annahmen über die Interessen der Nutzer werden anhand der Themen der angewählten Websites getroffen. Darüber hinaus hält Doubleclick fest wie oft eine Anzeige einem bestimmten Benutzer gezeigt wurde und ob der Nutzer darauf reagierte. All dies ermöglicht einmalige Dienste; z.B. kann eine Firma angeben, daß sie ihre Anzeige höchstens "x"-mal einem Nutzer gezeigt haben möchte. Oder die Nutzer können gezielt, durch Analyse ihrer Domännamen, branchenspezifische Werbung gezeigt bekommen.

Das System braucht weniger als 20 Millisekunden um festzustellen welche Anzeige eingefügt werden soll und es verfolgt über zehn Millionen Nutzer pro Monat durchs Web [Netscape (2) 1998]. Wenn man die [Altavista-Suchmaschine](#) aufruft, kann man in der Statuszeile beobachten, wie der Doubleclick-Server, ad.doubleclick.net, kontaktiert wird, um die aktuelle Anzeige für den Banner zu holen, der direkt unter der Eingabe plaziert ist.

Daher rührt auch der schlechte Ruf der Cookies. Abgesehen davon, daß diese normalerweise ohne Wissen des Kunden auf dessen Rechner abgelegt werden, stört die Surfer das Gefühl, daß "big brother" sie beobachtet. Es gibt inzwischen einige Möglichkeiten um das Speichern von Cookies zu verhindern:

- Die o.g. Methode dem Browser das Speichern von Cookies zu verbieten.
- Den Inhalt der Cookie-Datei löschen und die Eigenschaft: "schreibgeschützt" aktivieren.
- Programme wie [Cookiecutter](#), die das Setzen aller Cookies zulässt, aber nur nach Erlaubnis des Surfers den Inhalt an den Server zurück sendet. Dies hat den Vorteil, daß der Surfer Websites wie z.B. ein Bestellsystem, für die Cookies wichtig für die Funktionsfähigkeit sind, voll ausnutzen kann.
- Programme wie [Cookie Pal](#), die es dem Surfer erlauben Listen zu führen über Sites, die Cookies setzen oder nicht setzen dürfen.
- Websites wie [The Anonymizer](#), die ähnlich wie ein Proxy-Server agieren. Die eigene Domäne wird vor dem Protokollieren geschützt.

Eine Website die Cookies benutzt sollte dies auch angeben und ihre Nutzung erklären. Außerdem sollten keine wichtige Informationen wie Paßwörter unverschlüsselt in einem Cookie gespeichert werden, da vielleicht auch andere Leute Zugang zu dem Rechner des Surfers haben. Das würde vielleicht helfen, den schlechten Ruf von Cookies zu bekämpfen. Letztendlich hat der Surfer mit der neuen Browser-Generation vielfältige Möglichkeiten um selber zu bestimmen welche Cookies gesetzt werden und welche nicht.

Das WWW-Consortium (W3C) möchte mit dem Projekt ["Platform for Privacy Preferences Project" \(P3P\)](#) ein System schaffen, das zwischen allen Beteiligten einen offenen und durchschaubaren Interessenausgleich vermittelt. Die klammheimliche Datenerhebung soll verhindert werden und die Anbieter sollen gezwungen werden, die Privatsphäre der Surfer zu respektieren.

Die einfachste Art der Transaktion stellt der Austausch von digitalen Visitenkarten zwischen dem Diensteanbieter und dem Nutzer dar. Dabei handelt es sich schlicht um Dateien die Profilangaben im RDF-Format enthalten. Das Profil des Anbieters enthält neben Angaben zum Anbieter, die Site Practices, jene Regeln und Anforderungen, denen die Nutzung des Angebots unterliegt. Der Nutzer kann sich eine Vielzahl unterschiedlicher Profile erstellen.

Trifft ein P3P-Nutzer auf eine P3P-Website, so werden Profile ausgetauscht. Wenn die Profile übereinstimmen (die Neugier des Anbieters und den Offenbarungswillen des Surfers) wird der Zugang augenblicklich gewährt. Andernfalls tritt eine Art Verhandlungsphase ein. Der Surfer kann sich die Site Practices ansehen und entscheiden ob er die geforderten Informationen preisgeben möchte. Gleichfalls kann der Anbieter seine Anforderungen lockern und dem Surfer einen Testzugang erlauben.

P3P sieht Signaturen auf Anbieterseite vor, um Surfer vor Anbietern mit vorgetäuschten Identität zu schützen. Von besonderer Wichtigkeit wird auch die Kontrolle der Anbieterpraktiken sein: Wer persönliche Daten preisgibt, nur um mailwendend unerwünschte "Reichwerden-in-zwei-Stunden"-Angebote zu erhalten, muß sich bei einer Stelle beschweren können, die dem Anbieter auch mit Sanktionen drohen kann.

Dieses System erlaubt dem Nutzer die Grenzen seiner Privatsphäre von Fall-zu-Fall auf eindeutige und wirkungsvolle Weise festzulegen. [c't 6/98, S. 168]

C Literaturverzeichnis

| | |
|-------------|---|
| [c't 11/97] | Michael Wasmeier "Shop in the Box" in c't Magazin für Computer Technik 13.10. – 26.10.97 Heise, 1997, Hannover |
| [c't 13/97] | Wolfgang Tillmann, Dušan Zivadinovic "Mehrwertmedium – Das Fernsehkabel als Datenspediteur" in c't Magazin für Computer Technik 10.11. – 23.11.97 Heise, 1997, Hannover |
| [c't 16/97] | Axel Kossel, Hans-Jürgen Wronski "Bare Bytes – Online bezahlen im Internet" in c't Magazin für Computer Technik 22.12.97 – 04.01.98 Heise, 1997, Hannover |

| | |
|-----------------|---|
| [c't 06/98] | Michael Wilde "Stahlharte Kommerzwelle" in c't Magazin für Computer Technik 16.03. – 29.03.98 Heise, 1998, Hannover |
| [c't 09/98] | Dirk Brenken "Virtuelle Rathäuser" in c't Magazin für Computer Technik 27.04. – 10.05.98 Heise, 1998, Hannover |
| [c't 09/98 (2)] | Christiane Schulzki-Haddouti "Steuer fürs Internet" in c't Magazin für Computer Technik 27.04. – 10.05.98 Heise, 1998, Hannover |
| [c't 11/98] | Michael Wasmeier "Web-Währungen – Online-Bezahlungsverfahren für ECommerce" in c't Magazin für Computer Technik 25.05. – 07.06.98 Heise, 1998, Hannover |
| [c't 11/98 (2)] | Axel Kossel "Einkaufsbummel durchs Netz" in c't Magazin für Computer Technik 25.05. – 07.06.98 Heise, 1998, Hannover |
| [c't 15/98] | "Stoff aus dem Internet fürs papierlose Buch" in c't Magazin für Computer Technik 20.07. – 02.08.98 Heise, 1998, Hannover |
| [c't 16/98] | "Zandvoort und die Folgen" in c't Magazin für Computer Technik 03.08. – 16.08.98 Heise, 1998, Hannover |
| [c't 16/98 (2)] | "Grobschnitt" in c't Magazin für Computer Technik 03.08. – 16.08.98 Heise, 1998, Hannover |

| | |
|------------------|---|
| [CZ 27 1998] | "Die Key-Hinterlegung soll den Staat vor einem Krypto-Mißbrauch schützen" in Computer Zeitung Nr. 27 02.07.98 Konradin, 1998, Leinfelden |
| [CZ 28 1998] | "Business-Nutzung kommt in Fahrt" in Computer Zeitung Nr. 28 09.07.98 Konradin, 1998, Leinfelden |
| [CZ 28 (2) 1998] | "Die deutsche Kryptographiepolitik fährt trotz des Wahlkampfs einen liberalen Kurs" in Computer Zeitung Nr. 28 09.07.98 Konradin, 1998, Leinfelden |
| [CZ 31 1998] | "Agent-Einkäufer zwingen Online-Läden zu Preisabsprachen und Kartellbildung" in Computer Zeitung Nr. 31 30.07.98 Konradin, 1998, Leinfelden |
| [CZ 32 1998] | "Dolmetscher geleitet den Surfer ins Web" in Computer Zeitung Nr. 32 06.08.98 Konradin, 1998, Leinfelden |
| [CZ 34 1998] | "Europa entert den Cyberspace" in Computer Zeitung Nr. 34 20.08.98 Konradin, 1998, Leinfelden |
| [CZ 34 (2) 1998] | "Dell steht mit ihrem Erfolg beim Online-Verkauf allein auf weiter Flur" in Computer Zeitung Nr. 34 20.08.98 Konradin, 1998, Leinfelden |
| [CZ 36 1998] | "Kurz Notiert: Steuern" in Computer Zeitung Nr. 36 03.09.98 Konradin, 1998, Leinfelden |

| | |
|------------------|--|
| [CZ 36 (2) 1998] | "Das Trustcenter setzt den Schlußstein auf das virtuelle Dienstleistungsgebäude" in Computer Zeitung Nr. 36 03.09.98 Konradin, 1998, Leinfelden |
| [CZ 37 1998] | "USA suchen neuen Kryptostandard" in Computer Zeitung Nr. 37 10.09.98 Konradin, 1998, Leinfelden |
| [Doberenz 1998] | Walter Doberenz, Uwe Druckenmüller "Java Programmierung interaktiver WWW-Seiten" Hanser, 1998, München |
| [Dreyer 1998] | Wolfgang Dreyer, Harald Summa(Hrsg.) "Internet Business Online-Marketing, Electronic Commerce und Intranet" Interest, 1998, Augsburg |
| [Fochler 1998] | Klaus Fochler, Primož Perc, Jörg Ungermann "Electronic Commerce mit Lotus Domino" Addison-Wesley, 1998, Bonn |
| [Ghosh 1998] | Anup K. Ghosh "E-Commerce Security: Weak Links, Best Defenses" Wiley, 1998, USA |
| [Jepson 1997] | Brain Jepson "Java Database Programming Master Next Generation Web Database Techniques" Wiley, 1997, USA |
| [Kracke 1996] | Ulrich Kracke "Datenbank-Management" Interest, 1996, Augsburg |
| [Krüger 1998] | Thomas Krüger, Joachim Funke "Psychologie im Internet Ein Wegweiser für psychologisch interessierte User" Beltz, 1998, Weinheim |

| | |
|-------------------|--|
| [Kurbel 1998] | Prof. Dr. Karl Kurbel, Dipl.-Kfm. Frank Teuteberg "Betriebliche Internet-Nutzung in der Bundesrepublik Deutschland – Ergebnisse einer empirischen Untersuchung" Arbeitsbericht, 2., erweiterte Auflage, April 1998 http://curie.euv-frankfurt-o.de:8889/beitr/ab-empdisk.html |
| [Levine 1995] | Margaret Levine Young, John R. Levine "Internet FAQs" IDG, 1995, California, USA |
| [Münz 1997] | Stefan Münz "HTML-Dateien selbst erstellen Das Kompendium für Entwickler von WWW-Seiten" Version 6.1, 1997 http://www.teamone.de/selfhtml/ |
| [Rüdiger 1995] | Heinz-Rüdiger Huly, Stefan Raake "Marketing online Gewinnchancen auf der Datenautobahn" Campus, 1995, Frankfurt |
| [Schultz 1997] | Paul Schultz "Java 1.1 Schnell und sicher zum Ziel" Markt & Technik, 1997, München |
| [Stolpmann 1997] | Markus Stolpmann "Elektronisches Geld im Internet" O'Reilly, 1997, Köln |
| [Werner 1997] | Andreas Werner, Ronald Stephan "Marketing Instrument Internet" dpunkt, 1997, Heidelberg |
| [Zimmermann 1997] | Philip Zimmermann "PGP Pretty Good Privacy Das verschlüsselungsprogramm für Ihre private elektronische Post" FoeBuD e.V., 1997, Bielefeld |

D Websites

| | |
|------------------|---|
| [Cookie 1998] | http://www.cookiecentral.com |
|------------------|---|

| | |
|------------------------|---|
| [Deutsche 1998] | http://www.deutsche-bank.de |
| [IBM 1998] | http://www.ibm.com/e-business/de/ |
| [Karstadt 1998] | http://www.myworld.de |
| [Macrotron 1998] | http://www.macrotron.de |
| [Netscape 1998] | http://developer.netscape.com/docs/manuals/communicator/jsguide4/index.htm |
| [Netscape (2) 1998] | http://www.netscapeworld.com/nw-04-1997/nw-04-cookies.html |
| [NW 1998] | http://www.nw.com (Network Wizards) |
| [Peapod 1998] | http://www.peapod.com |
| [RIPE 1998] | http://www.ripe.net/statistics/hostcount.html |
| [W3B 1998] | http://www.w3b.de/ergebnisse/w3b6/ergebnisse.html |
| | http://altavista.digital.com |
| | http://java.sun.com:80/docs/books/tutorial/index.html |
| | http://www.alleykatt.com/coders |
| | http://www.amazon.com |
| | http://www.annonce.de |
| | http://www.anonymizer.com |
| | http://www.business-online.de/bo/umfrage/index.html |
| | http://www.cybercash.com |
| | http://www.dell.com |

| | |
|--|---|
| | http://www.deshima.de |
| | http://www.deutsche-bank.de/wwwforum/ecash/merchant/m_mall.htm |
| | http://www.developer.com |
| | http://www.digicash.com/ecash/ecash-home.html |
| | http://www.fv.com |
| | http://www.germany-service.com |
| | http://www.icat.co.uk |
| | http://www.industrienet.de |
| | http://www.infohiway.com/javascript/indexf.htm |
| | http://www.intershop.de |
| | http://www.itm.com/cgicollection |
| | http://www.javaworld.com |
| | http://www.kburra.com |
| | http://www.kohlhage.wlwonline.de |
| | http://www.medienparadies.de |
| | http://www.nasa.gov |
| | http://www.odci.gov/cia |
| | http://www.pgp.com |
| | http://www.research.ibm.com/infoecon/paps/html/alife6/alife6_public.html |
| | http://www.shopbot.com |
| | http://www.shopfido.com |
| | http://www.w3.org/P3P/overview.html |
| | http://www.web.de |

E Abkürzungsverzeichnis

| | |
|---------|--|
| EDI | Electronic Data Interchange |
| ADSL | Asymmetric Digital Subscriber Line |
| AES | Advanced Encryption Standard |
| AGBG | Gesetz zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen (AGB-Gesetz) vom 09.12.976 |
| API | Application Programming Interface |
| ARPAnet | Advanced Research Projects Agency net |
| ASIC | Application Specific Integrated Circuit |
| BfV | Bundesamt für Verfassungsschutz |
| BGB | Bürgerliches Gesetzbuch vom 18.08.1896 |
| BND | Bundesnachrichtendienst |
| CAD | Computer Aided Design |
| CCC | Chaos Computer Club |
| CGI | Common Gateway Interface |
| CIA | Central Intelligence Agency |
| CR | Computer und Recht (Zeitschrift) |
| DENIC | Deutsches Network Information Center |
| DES | Data Encryption Standard |
| DNS | Domain Name System |
| DoD | Department of Defence Amerikanisches Verteidigungsministerium |
| DIHT | Der Deutsche Industrie- und Handelstag |
| EGBGB | Einführungsgesetz zum Bürgerlichen Gesetzbuche vom 21.09.1994 |
| EZB | Europäischen Zentralbank |

| | |
|---------|--|
| FAQ | Frequently asked Questions Eine Zusammenstellung der meist gestellten Fragen und Antworten zu einem Thema |
| FBI | Federal Bureau of Investigation |
| FPGA | Field Programmable Gate Array |
| FTP | File Transfer Protocol |
| HBCI | Home Banking Computer Interface |
| HBV | Gewerkschaft Handel, Banken, Versicherungen |
| HTML | Hypertext Markup Language |
| HTTP | Hypertext Transport Protocol |
| ID | Identifikation, der Nutzernamen |
| IDEA | International Data Encryption Algorithm Ein Algorithmus für die symmetrische Verschlüsselung |
| IETF | Internet Engineering Task Force |
| IRC | Internet Relay Chat |
| ISDN | Integrated Services Digital Network |
| ISP | Internet Service Provider |
| InfoKDG | Informations- und Kommunikationsdienstegesetzes vom 22.07.1997 |
| JDBC | Wird fälschlicherweise für ein Akronym für "Java Database Connectivity" gehalten |
| JDK | Java Development Kit |
| LG | Landgericht |
| MD5 | Message Digest 5 Ein Algorithmus um Textprüfsummen zu erzeugen |
| MILnet | Military net |
| NASA | National Aeronautics and Space Administration |
| NIST | National Institute of Standards and Technology |

| | |
|----------|--|
| NOC | Network Operations Centre |
| NSF(net) | National Science Foundation (net) |
| OECD | Organisation for Economic Co-operation and Development |
| ODBC | Open Database Connectivity (Schnittstelle für relationale Datenbanken) |
| P3P | Platform for Privacy Preferences Project |
| PGP | Pretty Good Privacy Verschlüsselungsprogramm |
| RIPE NCC | Réseaux IP Européens Network Coordination Centre. Ziel der RIPE ist es die administrative und technische Koordination des Netzes in Europa zu sichern |
| RSA | |
| SET | Secure Electronic Transaction Protokoll zur geschützten und authentischen Übertragung von Zahlungsinformationen über offene Netze. |
| SigG | Signaturgesetz, Artikel 3 IuKDG |
| SQL | Structured Query Language |
| TDDSG | Teledienstedatenschutzgesetz, Artikel 2 IuKDG |
| TDG | Teledienstegesetz, Artikel 1 IuKDG |
| UDSL | Universal Digital Subscriber Line |
| URL | Uniform Resource Locator |
| VerbrKrG | Verbraucherkreditgesetz vom 17.12.1990 |
| W3C | WWW-Consortium |
| WWW | World Wide Web |

F Tabellen- und Abbildungsverzeichnis

Tabelle 1: Zweck der WWW-Nutzung

Tabelle 2: WWW zum Shopping nutzen

| | |
|-------------|--|
| Tabelle 3: | WWW erneut zum Shopping |
| Tabelle 4: | Beispieldatei "form.htm" |
| Tabelle 5: | Beispieldatei "comments.pl" |
| Tabelle 6: | Beispieldatei "check.htm" |
| Tabelle 7: | Beispieldatei "test.htm" |
| Tabelle 8: | Beispieldatei "Test.java" |
| Tabelle 9: | Auszug aus der Artikeldatenbank von Kohlhage |
| Tabelle 10: | Inhalt eines VALUE Tags in data.htm |
| Tabelle 11: | Die Felder eines Cookies |
| Tabelle 12: | Bezahlung von Leistungen über das WWW |
| Tabelle 14: | Sicherheit symmetrischer Schlüssel |
| Tabelle 15: | Ein mit PGP verschlüsselter Text |

| | |
|---------------|---|
| Abbildung 1: | Optionen im E-Commerce |
| Abbildung 2: | Verteilung der Online-Präsenzen auf die Wirtschaftszweige |
| Abbildung 3: | Phase 1 der Online-Bestellung |
| Abbildung 4: | Phase 2 der Online-Bestellung |
| Abbildung 5: | Phase 3 der Online-Bestellung |
| Abbildung 6: | Hierarchische Struktur der Website |
| Abbildung 7: | Ablauf einer Kundenbestellung |
| Abbildung 8: | Startmaske des Bestellsystems |
| Abbildung 9: | Aufbereitete Artikeldaten |
| Abbildung 10: | Der Warenkorb |
| Abbildung 12: | Bildschirm zur Auslösung einer Bestellung |
| Abbildung 13: | Symmetrische Kryptographie |
| Abbildung 14: | Asymmetrische Kryptographie |
| Abbildung 15: | Asymmetrische Kryptographie als digitale Unterschrift |
| Abbildung 16: | Kombination symmetrische/asymmetrische Kryptographie |
| Abbildung 17: | Verschlüsselung mit PGP |
| Abbildung 18: | Protokoll-Stack für Internet Kommunikation |
| Abbildung 20: | Die Framestruktur der Website |

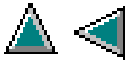
G Glossar

| | |
|----------|--|
| Extranet | Eine Verbindung des Intranets eines Unternehmen zu denen der Zulieferer und Abnehmer |
|----------|--|

| | |
|------------------------|--|
| Active content | Dynamische, interaktive Ergänzung einer HTML-Seite |
| Applet | Eine Java-Programm, das mit einem Java-fähigen Browser oder einem Applet Viewer läuft. |
| Banner | Kleine anklickbare Werbegrafiken. |
| Business Netiquette | "Knigge" für den Umgang mit Geschäftspartnern im ECommerce |
| comma-seperated-values | Eine Datensammlung (Datenbank) deren Spalten durch Zeichen wie Semikola und Zeilen durch Zeilenvorschübe getrennt werden. |
| Digitale Signatur | Elektronische Unterschrift |
| Disintermediation | Die Ausschaltung des Mittelmannes; Der Hersteller bzw. Großhändler verkauft an der Endverbraucher |
| Domäne | Einen aus mehreren Teilen bestehende Name, der einen Rechner im Internet identifiziert. |
| Downstream | Der Datenfluß vom Provider zum Kunden, Empfangsrichtung |
| Firewall | Eine Firewall ist ein Rechner, der wie eine schützende Mauer zwischen dem firmeninternen Netzwerk und dem Internet selbst liegt. |
| Mall | Einkaufszentrum |
| Micropayments | Online-Zahlungen die einen Wert zwischen einigen Pfennigen und fünf Mark besitzen. (In den USA: zwischen 25 cents und 10\$) |
| Netizens | Net citizens, Internet Nutzer |
| One-to-One Marketing | Eine Marketingstrategie bei der die Kunden gezielt individuell angesprochen werden. |
| Plug-in | Utility, das einen Browser ergänzt, indem es über eine definierte Schnittstelle neue Funktionen zur Verfügung stellt. |
| Server | Ein Computer der anderen Computern, den Clients, bestimmte Dienste anbietet. |
| Smartcards | Chipkarten |
| Storefront | Die Einstiegsseite eines virtuellen Ladens. |

| | |
|-------------------------|---|
| Certification Authority | Quasi notarielle Organisationen, die als Zertifizierungsstellen auftreten und die Zusammengehörigkeit von Public-Key und Besitzer gewährleisten. Dies ist notwendig um, um authentischen, vertraulichen und anonymen Datenverkehr zu garantieren. |
| Upstream | Der Datenfluß vom Kunden zum Provider, Senderichtung |
| Web Directory | Gelbe Seiten ähnliche Verzeichnisse von Web Seiten |

¹Frühere Browser erlaubten nur die Einstellungen: entweder alle Cookies akzeptieren oder keine.



Welcome to
Peapod
*Online grocery shopping
and delivery.*



Already a customer?

[Please Login](#)

Username:

Password:

[Save my username & password](#)

New to Peapod?



**Groceries for
your home**



**Groceries for
your business**

© 1990-2002 Peapod, Inc. All rights reserved.